Buyer's Guide: Enterprise SSDs p. 57

Windows® IT Pro

A PENTON PUBLICATION

NOVEMBER 2011 | WINDOWSITPRO.COM | WE'RE IN IT WITH YOU

WINDOWS EVOLVED

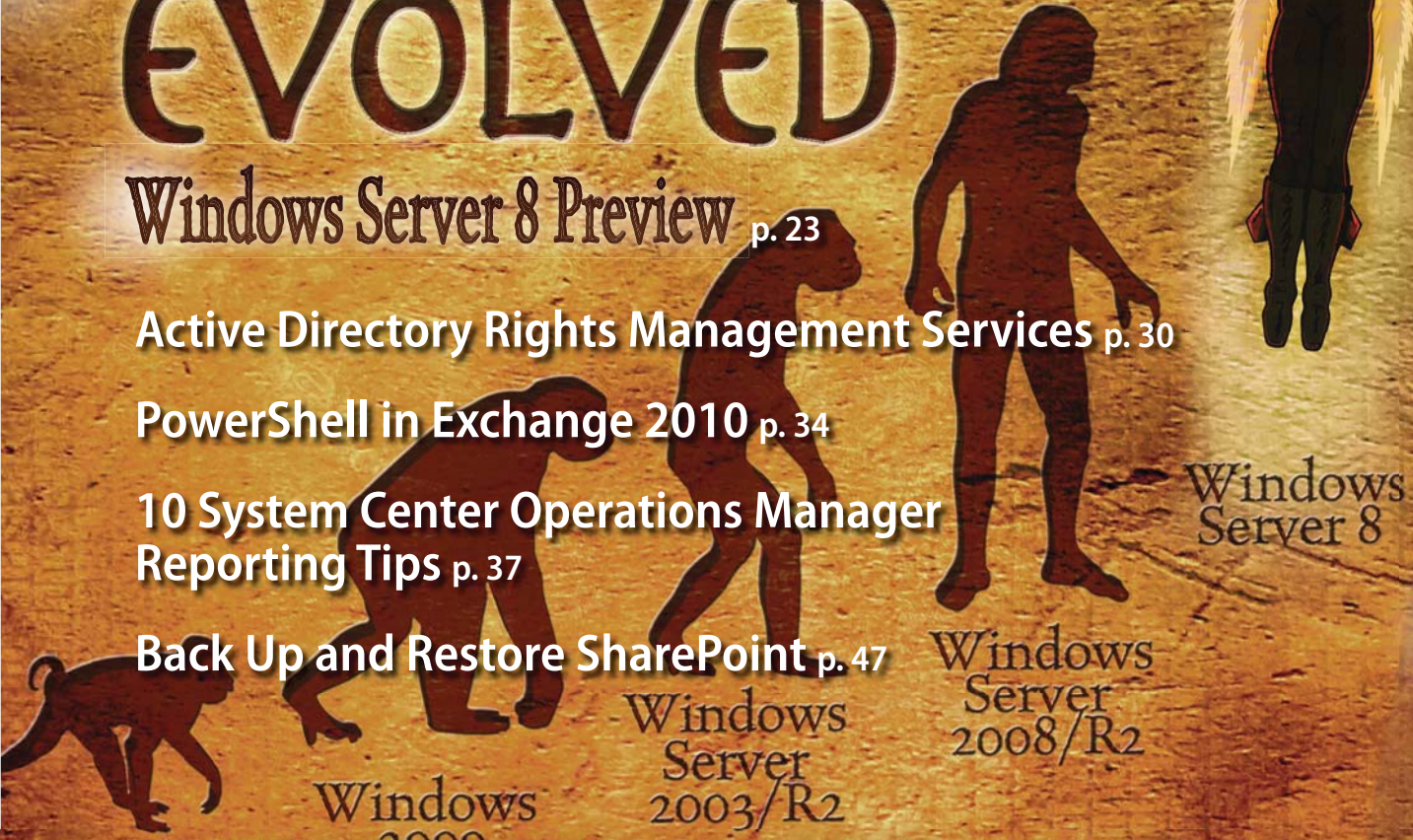
Windows Server 8 Preview p. 23

Active Directory Rights Management Services p. 30

PowerShell in Exchange 2010 p. 34

10 System Center Operations Manager Reporting Tips p. 37

Back Up and Restore SharePoint p. 47



Systems Administrator of the Year p. 5

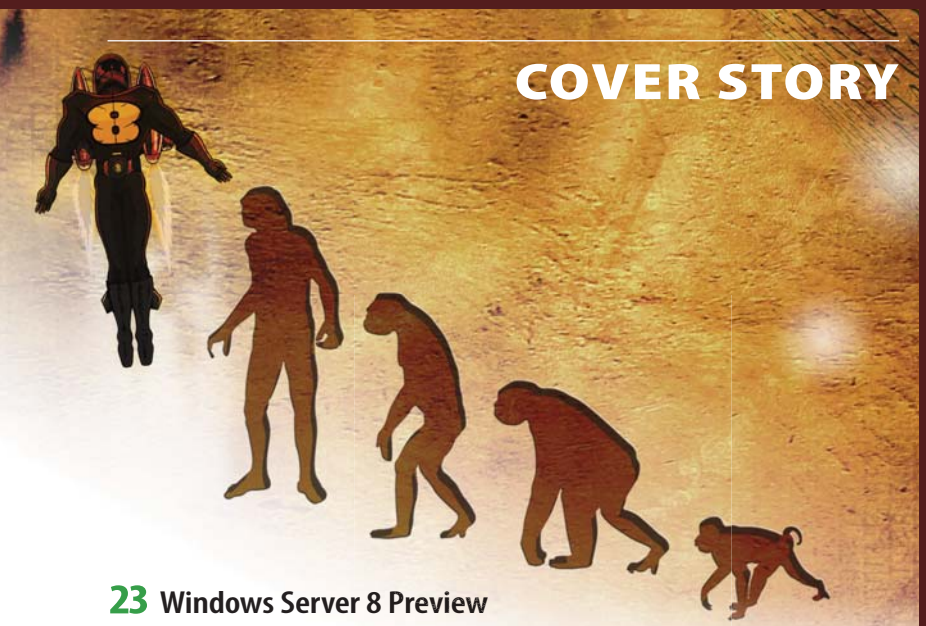
DB2 on POWER: 3x faster. Check. As low as 1/3 the price. Mate.

Which database has the right moves? DB2® on Power Systems™ performs three times faster per core than Oracle Database on SPARC—based on both TPC-C and SAP® SD benchmarks.* Yet the price of DB2 is as low as 1/3 the price of Oracle Database.** Maybe that's why in 2010 over 1,000 Oracle Database clients chose DB2 instead. Game over.

ibm.com/facts

*PERFORMANCE: www.tpc.org as of 3/28/11 [IBM Power 780 (3 x 64 C)(24 Ch/192 C/768 Th); 10,366,254 tpmC; $1.38/tpmC; avail. 10/13/10 v. Oracle SPARC SuperCluster w/T3–4 Servers (27 x 64 C)(108 Ch/1728 C/13824 Th); 30,249,688 tpmC; $1.01/tpmC; avail. 6/1/11]. TPC-C is a trademark of Transaction Performance Processing Council. 2-tier SAP SD standard application benchmark results as of 3/28/11 [IBM Power 795 (32 P/256 C/1024 Th); 126,063 users, SAP ERP 6.0 EhP4/AIX 7.1 + DB2 9.7; cert. 2010046 v. Oracle SPARC Enterprise Server M9000 (64 P/256 C/512 Th); 39,100 users, SAP ERP 6.0/Solaris 10, Oracle 10g; cert. 2008042] www.sap.com/benchmark. SAP and all SAP logos are trademarks or registered trademarks of SAP AG in Germany and several other countries. **PRICE: based on publicly avail. U.S. info on 2/10/2011 for IBM DB2 Advanced Enterprise Edition + Oracle software w/comparable capabilities. No SAP SD benchmark results are used for any price/performance metrics. IBM: 100 Processor Value Units. Oracle: assumes 1.0 processor multiplier. Both incl. Y1 maint./support. IBM, the IBM logo, ibm.com, DB2, Power Systems, Smarter Planet and the planet icon are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml.

CONTENTS



COVER STORY

23 Windows Server 8 Preview

Windows IT Pro authors share their first impressions of Windows Server 8 after Microsoft's BUILD conference and the Windows Server 8 Reviewers Workshop. Paul Thurrott gives you the mile-high view, Sean Deuby covers Active Directory, Jeff James focuses on storage, and Michael Otey discusses virtualization.

BY PAUL THURROTT

FEATURES

30 Active Directory Rights Management Services

Microsoft Windows Rights Management Services (RMS) provides four options for exchanging RMS-protected documents between organizations. Learn how to use AD RMS for secure collaboration between you and your partners.

BY JAN DE CLERCQ

34 What's New: Exchange Server 2010 & Remote PowerShell

Changes to Microsoft Exchange Server's Exchange Management Shell (EMS) in Exchange 2010 are significant because EMS is so crucial to Exchange management. Learn how to use PowerShell effectively in Exchange 2010.

BY PAUL ROBICHAUX

37 10 System Center Operations Manager Reporting Tips

Microsoft System Center Operations Manager provides the necessary framework for extremely powerful and flexible reporting; however, Operations Manager is also unintuitive and difficult to use. These 10 tips will help you make the most of Operations Manager's capabilities.

BY CAMERON FULLER

43 Renaming Scheduled Tasks in Windows 7, Server 2008, and Vista

Walk through a Windows PowerShell script that renames Task Scheduler tasks in Windows 7, Windows Server 2008, and Windows Vista.

BY BILL STEWART

47 Backing Up SharePoint Content, Configurations, and Components

The wide array of tools to back up and restore a SharePoint environment can be quite daunting. A good place to start is to use SQL Server's backup and restore tools and the SharePoint 2010 Management Shell in addition to the backup and restore options in SharePoint's Central Administration site.

BY MICHAEL NOEL

INTERACT

16 Reader to Reader

Find out how to avoid the latest crop of viruses that are disguised as antivirus programs and how to configure your security software's text messages to make troubleshooting easier.

19 Ask the Experts

See Outlook 2010's Backstage view, learn how to let non-administrators perform activation actions, and get info on virtualization, systems management, encryption key storage, data center bridging, and yes, Xbox 360.

IN EVERY ISSUE

7 IT Community Forum

63 Directory of Services

63 Advertising Index

63 Vendor Directory

64 Ctrl+Alt+Del

Access articles online at www.windowsitpro.com. Enter the article ID (located at the end of each article) in the Search box on the home page.

Windows IT Pro
A PENTON PUBLICATION

NOVEMBER 2011
VOLUME_17 NO_11

COLUMNS

JAMES | IT PRO PERSPECTIVES

4 Reimagining Microsoft

Microsoft's new server and client OSs, Windows Server 8 and Windows 8—which include improvements to the UI, Hyper-V, Active Directory, and storage—promise to help the software giant gain some ground against competitors.

SYSTEMS ADMINISTRATOR OF THE YEAR

5 2011 Systems Administrator of the Year: John Wischmeier

John Wischmeier shared his solution to a particularly tough communications problem and took the grand prize in our first annual Systems Administrator of the Year contest.

THURROTT | NEED TO KNOW

10 Windows 8 and Windows Server 8 Reimagining, and Whither Windows Phone?

Windows Server 8 is a huge upgrade for businesses—one that will have ramifications a decade down the road. Learn how it might affect you.

MINASI | WINDOWS POWER TOOLS

12 Go Remote with Windows Server 2008 R2's AD Cmdlets

Active Directory–related PowerShell cmdlets provide for remote administration.

OTEY | TOP 10

13 Windows 7 Productivity Tips

These Windows 7 tips show how the many new or upgraded features of Microsoft's latest desktop OS can increase productivity. Learn to use Jump Lists, speech recognition for voice commands, and how to clean up your start-up programs list.

DEUBY | ENTERPRISE IDENTITY

14 Is Your Identity and Access Infrastructure Ready for the Cloud?

The Office 365 Deployment Readiness Tool is a free, easy-to-use utility that gives you a quick assessment of your Active Directory, Exchange Server, and SharePoint environment.

C O N T E N T S

PRODUCTS

50 New & Improved
Check out the latest products to hit the marketplace.
PRODUCT SPOTLIGHT: **VMware Fusion 4** and **VMware Workstation 8**.

REVIEW
51 Paul's Picks
See why Windows 8's UI is so successful that Microsoft is using it in other products; plus, learn why Small Business Server 2011 Essentials is almost, but not quite, a no-brainer for SMBs.
BY PAUL THURROTT

REVIEW
52 ExtremeZ-IP
This Mac OS X integration tool is easy to deploy yet very complete in its ability to integrate Macs into a Windows Active Directory environment.
BY NATE MCALMOND

REVIEW
54 Social Sites for SharePoint 2010
Social Sites extends an existing SharePoint 2010 deployment to add a host of collaborative social media functions. This in-house social media toolset is highly complex but incredibly useful and powerful.
BY JOHN HOWIE

REVIEW
55 ToughTech mini-Q
This external hard drive is a good choice if you're looking for a solution for sensitive files and documents that's more secure than other removable backup options.
BY JEFF JAMES

BUYER'S GUIDE
57 Enterprise SSDs
Solid state disk (SSD) drives offer significant advantages and disadvantages to your storage scenario. This buyer's guide provides some key points to keep in mind.
BY JASON BOVBERG

60 Industry Bytes
Yale University student information was inadvertently made accessible through Google search, Michael B. Smith discusses trends for Exchange Server 2010 deployments, and Orin Thomas discusses how systems administrators should prioritize their tasks.

Windows IT Pro

EDITORIAL

Editor in Chief
Amy Eisenberg amy@windowsitpro.com

Senior Technical Director
Michael Otey motey@windowsitpro.com

Technical Director
Sean Deuby sean@windowsitpro.com

Senior Technical Analyst
Paul Thurrott paul@windowsitpro.com

Industry News Analyst
Jeff James jjames@windowsitpro.com

Custom Group Editorial Director
Dave Bernard dbernard@windowsitpro.com

Exchange & Outlook
Brian Winstead bwinstead@windowsitpro.com

Systems Management, Networking, Hardware
Jason Bovberg jbovberg@windowsitpro.com

Security, Virtualization
Jeff James jjames@windowsitpro.com

SharePoint
Caroline Marwitz cmarwitz@windowsitpro.com

SQL Server, Developer Content
Megan Keller mkeller@windowsitpro.com

Managing Editor
Lavon Peters lavon.peters@penton.com

Editorial Assistant
Blair Greenwood blair.greenwood@penton.com

CONTRIBUTORS

SharePoint and Office Community Editor
Dan Holme danh@intelliem.com

Senior Contributing Editors
David Chernicoff david@windowsitpro.com
Mark Minasi mark@minasi.com
Paul Robichaux paul@robichaux.net
Mark Russinovich mark@sysinternals.com
John Savill john@savilltech.com

Contributing Editors
Alex K. Angelopoulos aka@mvps.org
Michael Dragone mike@mikerochip.com
Jeff Fellinge jeff@blackstatic.com
Brett Hill brett@iisanswers.com
Darren Mar-Elia dmarelia@windowsitpro.com
Tony Redmond 12knocksinna@gmail.com
Eric B. Rux ericbrux@whshelp.com
William Sheldon bsheldon@interknowlogy.com
Curt Spanburgh cspanburgh@scg.net
Orin Thomas orin@windowsitpro.com
Douglas Toombs help@toombs.us
Ethan Wilansky ewilansky@windowsitpro.com

ART & PRODUCTION

Production Director
Linda Kirchgesler linda@windowsitpro.com

Senior Graphic Designer
Matt Wiebe matt.wiebe@penton.com

ADVERTISING SALES

Publisher
Peg Miller pmiller@windowsitpro.com

Director of IT Strategy and Partner Alliances
Birdie J. Ghiglione birdie.ghiglione@penton.com
619-442-4064

Online Sales Development Director
Amanda Phillips amanda.phillips@penton.com

Key Account Director
Chrissy Ferraro christina.ferraro@penton.com
970-203-2883

Account Executives
Barbara Ritter barbara.ritter@penton.com
858-367-8058
Cass Schulz cassandra.schulz@penton.com
858-357-7649

Client Project Managers
Michelle Andrews 970-613-4964
Kim Eck 970-203-2953

Ad Production Supervisor
Glenda Vaught glenda.vaught@penton.com

MARKETING & CIRCULATION

Customer Service service@windowsitpro.com

IT Group Audience Development Director
Marie Evans marie.evans@penton.com

Marketing Director
Sandy Lang sandy.lang@penton.com

CORPORATE

PENTON

Chief Executive Officer
Sharon Rowlands sharon.rowlands@penton.com

Chief Financial Officer/Executive Vice President
Nicola Allais nicola.allais@penton.com

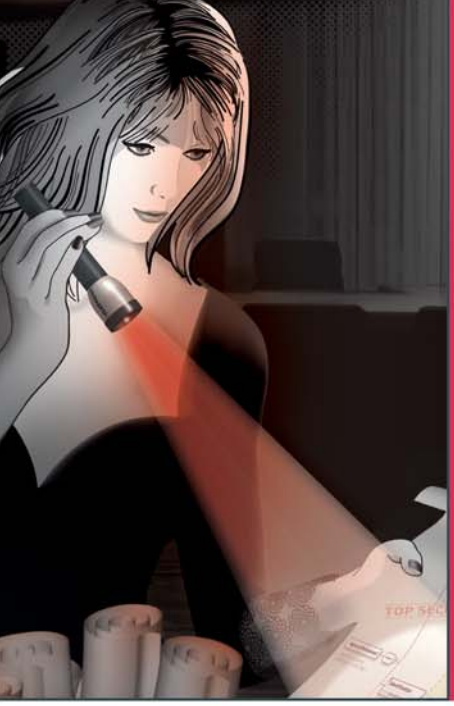
TECHNOLOGY GROUP

Senior Vice President, Technology Media Group
Kim Paulsen kpaulsen@windowsitpro.com

WRITING FOR *WINDOWS IT PRO*
Submit queries about topics of importance to Windows managers and systems administrators to articles@windowsitpro.com.

LIST RENTALS
Contact MeritDirect, 333 Westchester Avenue, White Plains, NY or www.meritdirect.com/penton.

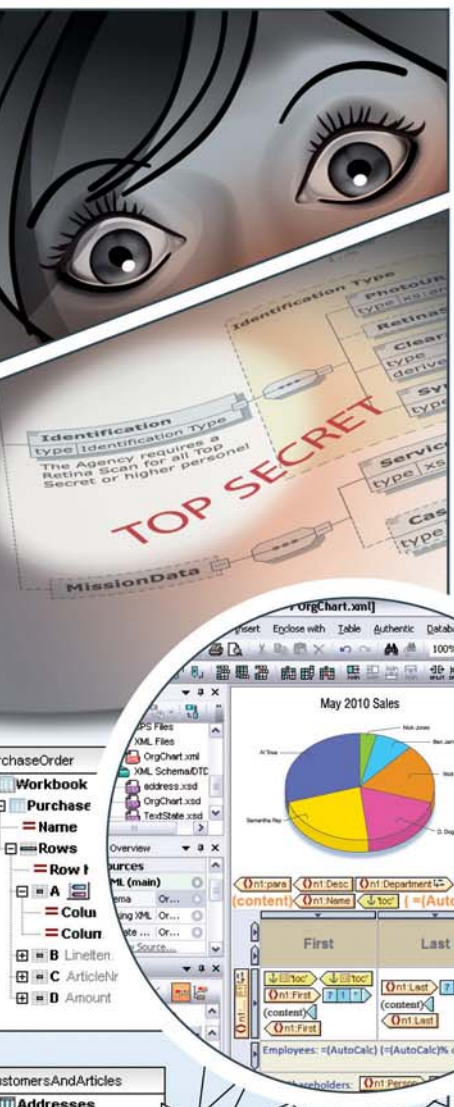
REPRINTS
reprints@pentonreprints.com, 888-858-8851

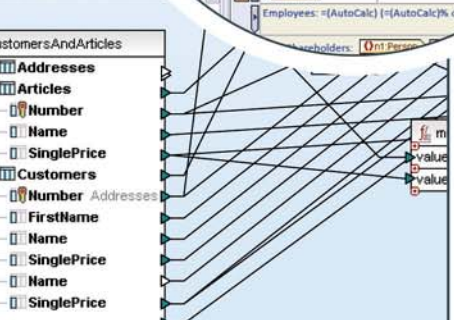


Bring your XML development projects to light with the complete set of tools from Altova®

ALTOVA® missionkit®

Experience how the Altova MissionKit®, the integrated suite of XML, database, and data integration tools, can simplify even the most advanced XML development projects.





The Altova MissionKit includes multiple intelligent XML tools:

XMLSpy® – industry-leading XML editor

- Support for all XML-based technologies
- Editing of HTML4, HTML5, XHTML, CSS
- Graphical editing views, powerful debuggers, code generation, & more

MapForce® – graphical data mapping & ETL tool

- Drag-and-drop data conversion with code generation
- Mapping of XML, DBs, EDI, Excel® 2007+, XBRL, flat files & Web services

StyleVision® – visual stylesheet & report designer

- Graphical stylesheet and report design for XML, XBRL & databases
- Report designer with chart creation
- Output to HTML, PDF, Word & eForms

Plus up to five additional tools…

Download a 30 day free trial!

Try before you buy with a free, fully functional, trial from **www.altova.com**

Scan with your smartphone to learn more about these products

James

"Microsoft could use some good news, after years of lurching from one uninspired product launch to another."

Reimagining Microsoft

How Windows 8 and Windows Server 8 change the rules

At Microsoft's recent BUILD conference, Microsoft President and CEO Steve Ballmer told BUILD attendees that he was delighted to hear how well the Windows 8 preview was being received. Ballmer said, "If Windows 8 is Windows re-imagined, we're also in the process of re-imagining Microsoft." Judging by what I and my *Windows IT Pro* colleagues have seen of Windows Server 8 and Windows 8 recently, Ballmer's comments might not have been far from the mark. Ballmer went on to say that Microsoft is reorganizing itself around four main priorities, including new hardware form factors (such as tablets and smartphones), cloud computing services, new application formats and delivery methods, and new developer tools and opportunities.

Microsoft could use some good news, after years of lurching from one uninspired product launch to another. Zune. Windows Vista. Kin. Windows Mobile. Lackluster Windows Phone 7 adoption. You can't argue with the success of Windows 7, but Microsoft was increasingly looking like a company that had lost the plot, a former industry giant plagued by sclerotic, innovation-killing bureaucracy and beset by more nimble and agile competitors. Ironically, Microsoft was beginning to look like the IBM that a young Microsoft out-foxed and out-innovated decades ago.

Like the US space program during the cold war, or American muscle car manufacturers, Microsoft seems to work best when facing a relentless adversary that seems to have gained the lead in the marketplace. The threat of Sputnik pushed the US space program to dizzying new heights, and the ongoing war of one-upmanship between the Ford Mustang, Chevrolet Camaro, and Dodge Challenger has resulted in a modern-day muscle car revival. Strong competition is good for consumers and separates strong companies with winning ideas and solid products from weak ones with bad ideas and uninspired products.

In Microsoft's case, that competition came in three forms: Google, Apple, and VMware. Google has the upper hand in cloud services and search; Apple has dominated the smartphone, tablet, and OS discussion; and VMware has been cleaning Microsoft's clock for years in the virtualization market. Windows 8 and Windows Server 8—and their supporting technologies, such as Windows Live SkyDrive—promise to help Microsoft gain some ground against all of these competitors, with Windows Server 8 delivering a host of new and improved cloud and virtualization technology, and the Metro interface employed in Windows 8 having the promise of finally offering a competitive touch-screen–centric alternative to Apple's iOS and iPad.

It might have a bloody nose, a black eye, and be down on points, but Microsoft seems to have finally decided it has spent enough time being the stumbling, disoriented, glass-jawed punching bag for Apple, Google, and VMware. Judging by what *Windows IT Pro* editors and contributors saw over the past few weeks, Redmond seems to have wiped the sweat from its eyes, spit some blood on the mat, and climbed back into the ring to do some damage. Microsoft is back in a big way, baby, and has some scores to settle.

Microsoft has put a lot of effort into Windows 8 and Server 8, and that effort shows: The new and improved feature list for Windows Server 8 runs into the hundreds, with massive enhancements to existing features (such as Hyper-V) and long-overdue upgrades to less flashy features—such as improvements to CHKDSK and IP address management—that will make Windows systems administrators more efficient and give them back some precious time. A few of our editors got some hands-on time with Windows 8 running on tablet devices, and the consensus is that Microsoft could potentially have a real iPad competitor on its hands. Granted, we likely won't see final versions of Windows Server 8 and Windows 8 until almost a year from now, but Microsoft is clearly making big bets and lavishing vast development resources on both products.

In this issue, we cover Windows Server 8 from many angles. Michael Otey looks at improvements to Hyper-V, Sean Deuby examines upgrades to Dynamic Access Control and Active Directory (AD), and I take a look at Windows Server 8 storage features. Paul Thurrott also provides his perspective on Windows Server 8. There's a lot of new material to cover with Windows Server 8 and Windows 8. Stay tuned for a flood of new coverage from us in the coming weeks and months that will describe all of the upcoming features of Windows 8 and Windows Server 8 in more detail.

InstantDoc ID 140625

JEFF JAMES (jeff.james@penton.com) is industry news analyst for *Windows IT Pro*. He was previously editor in chief of Microsoft *TechNet* magazine, was an editorial director at the LEGO Company, and has more than 15 years of experience as a technology writer and journalist.

2011 Systems Administrator of the Year: John Wischmeier

Windows IT Pro would like to congratulate John Wischmeier for taking the grand prize in our first annual Systems Administrator of the Year contest. More than 3,000 people voted in our survey, which presented essays from IT pros in which they described a heroic problem-resolution scenario that they spearheaded. In the end, more than 1,200 people catapulted John to the top of the heap in this contest, enjoying his essay about the way he tackled a particularly tough communications problem. Our 10 finalists were:

- Jon Anderson
- Warren Barton
- Dale Curren
- David T. Klein
- Chuck Lathorpe
- Christopher Nolan
- Jason Palm
- Paul Smith
- Michael Van Lare
- John Wischmeier

These 10 finalists were chosen by staff editors based on the following criteria: problem-solving creativity; cost savings; use of available and emerging technology; and business value. John's story hits a home run on all counts. Here's John's winning essay:

> My name is John Wischmeier. We have eight locations and require access to an outside vendor within our WAN infrastructure. Our existing MPLS circuit wasn't fast enough between a few of our locations, and the cost to upgrade the existing lines was out of reach. I shopped for a new provider and discovered that the outside vendor was only willing to work with our existing provider. That was discouraging, but I kept working on it with the hope of an answer. I found a new provider I was comfortable working with, but the solution they offered was very expensive, and we still needed to keep a line of communication to that outside vendor, which added even more expense to the proposition. Making it even more expensive was the idea that our outside vendor is critical to our business and we can't just have one connection to them. Everyone else had given up on the project, deciding that we were either going to have to pay a very high price, or we were going to have to sacrifice reliability and go with another vendor that didn't offer the redundancy we required. I just kept pushing forward, knowing there had to be a solution out there that fit us. One night, I was eating pizza with my family and I thought to myself, "If you can order a pizza with different toppings on the two halves, why can't you do the same thing with WAN infrastructure?" The next day, I called our existing vendor and asked if they could work with that, and I called the prospective vendor and asked them to put a plan together for me using those parameters. What I ended up with is an MPLS circuit with our existing provider that gives us the required redundant connection to our outside vendor, only connecting to three of our locations instead of all eight. I have another MPLS circuit with the new provider that is very high speed and has redundant paths between our locations. I then have an internal MPLS circuit that ties the other two together at multiple locations. I now have the best of both worlds: the connections I need to keep the business going with the added speed to efficiently get the job done—and we didn't have to sacrifice reliability; we actually improved it! My favorite part was telling the owner that I was able to accomplish this and, while doing so, lower our monthly communication expenses by 25 percent!

John's grand prize consists of the following:

- Xbox 360 + Kinect (donated by ScriptLogic)
- Apple iPad 2 (donated by Specops Software)
- Up to 100 Specops Deploy licenses (for the winner's employer)
- Windows Server 2008 MCITP Enterprise Admin Training Package (donated by TrainSignal)
- Exchange Server 2010 MCITP Training Package (donated by TrainSignal)

All 10 of our Systems Administrator of the Year finalists received the following:

- TrainSignal coffee mug
- Specops Software hat
- Up to 100 Specops Password Policy licenses (for their employer)
- *Windows IT Pro* prize package (t-shirt, tote bag, portable USB charger)

Congratulations to John and all of our finalists! Stay tuned next year for our second annual Systems Administrator of the Year contest, which will coincide with the official System Administrator Appreciation Day, July 27, 2012.

TOP 10

Bagley

"Independently reviewed by industry experts these free tools proved to be useful for IT pros."

Top 10 Free Tools for IT Professionals

New & Updated

Audit Active Directory and file servers, securely manage passwords, detect inactive users and more – for free.

Here is the updated list of freeware tools by NetWrix Corporation which can save you a lot of time and make your network more efficient – at absolutely no cost. All of these tools also have advanced commercial editions with additional features, but the freeware editions will not expire, and will not stop working when you urgently need them.

1 **UPDATED! Active Directory Change Reporter** (Windows IT Pro, Sep'09: InstantDoc ID 102446, TechRepublic: www.url2open.com/13) — This simple auditing tool keeps tabs on what's going on inside your Active Directory. The Windows IT Pro 2010 Community Choice and Editors' Best Award-winner tracks changes to users, groups, OUs, and all other types of AD objects, sending detailed daily reports with lists of changes. **Download page**: www.url2open.com/ADCRfree

2 **NEW! Password Manager** (Active Directory Tools, Jun '11: www.url2open.com/15)— A simple solution that gives the end users the ability to reset their forgotten passwords, troubleshoot account lockouts and unlock their accounts manually, through a secure web based interface, or a windows application that integrates with the Windows logon procedure. The new freeware version handles Google Apps, supports 10 languages and up to 50 users. **Download page:** www.url2open.com/PRMfree

3 **Password Expiration Notifier** (Redmond Magazine Feb'09, 4sysops: www.url2open.com/10)—This tool automatically reminds users to change their passwords before they expire, helping keep helpdesk administrators safe from password reset calls. It works nicely for users who don't log on interactively and, thus, never receive standard password change reminders at log on time (VPN and OWA). **Download page:** www.url2open.com/PENfree

4 **UPDATED! Privileged Account Manager** (TechRepublic Jul'11: www.url2open.com/16, SC Magazine: www.url2open.com/12)—This product maintains a repository of privileged user accounts (such as Administrator, root, service accounts etc) in Active Directory, servers, and other systems, providing a secure web-based portal for role-based access and automatic maintenance of shared administrative user accounts. The tool can automatically generate strong passwords at specified intervals (e.g. every 30 days) and synchronize password changes on all target systems (for example, change service account password in Active Directory and update service credentials). **Download page:** www.url2open.com/PAMfree

5 **Inactive Users Tracker** (MS TechNet Magazine May'08: www.url2open.com/20, TechRepublic: www.url2open.com/Z) — This tool tracks down inactive user accounts (e.g., terminated employees) so you can easily disable them, or even remove them entirely, thus eliminating potential security holes. The tool sends reports on a regular schedule, showing what accounts have been inactive for a configurable period of time (e.g., 2 months). **Download page:** www.url2open.com/IUTfree

6 **File Server Change Reporter** (4sysops.com: www.url2open.com/Y)—This is a must-have tool for auditing file servers and appliances. The tool detects changes made to files, folders and permissions, and tracks newly created and deleted files. The tool is useful for detecting mistakenly deleted files and it allows quick backup recovery of accidental changes. **Download page:** www.url2open.com/FSCRfree

7 **Active Directory Object Restore Wizard** (Windows IT Pro: www.url2open.com/X)—This tool can save the day if someone accidentally (or intentionally) deletes important Active Directory objects. It provides granular object-level, and even attribute-level restore capabilities that allow quick rollbacks of unwanted changes (e.g., mistakenly deleted users, modified group memberships, etc). **Download page:** www.url2open.com/ADRWfree

8 **Windows Service Monitor** (WindowsReference.com: www.url2open.com/U)—This very simple monitoring tool alerts you when some Windows service accidentally stops on one of your servers. The 2010 Windows IT Pro Community Choice and Editor's Best Award-winning tool also detects services that fail to start at boot time, which can happen, for example, with Microsoft Exchange. **Download page:** www.url2open.com/NSMfree

9 **Disk Space Monitor** (MS TechNet Magazine Sep'09: www.url2open.com/T)—Even with today's terabyte-large hard drives, server disk space tends to run out quickly and unexpectedly. This simple monitoring tool will send you daily reports regarding all servers that are running low on disk space, below the configurable threshold. **Download page:** www.url2open.com/DSMfree

10 **VMware Change Reporter** (TechTarget/SearchVirtualDesktop: www.url2open.com/V)—If you don't know what is being changed by your colleagues in the VMware infrastructure, it's very easy to get lost and miss changes that can affect things that you are responsible for. This 2010 Windows IT Pro Community Choice and Editor's Best Award-winner tracks and reports changes in VMware Virtual Center settings and permissions, such as newly created virtual machines, containers, alerts and more.
Download page: www.url2open.com/CRVMfree

JOHN BAGLEY (john_bagley@sbcglobal.net) is an award-winning professional writer and independent consultant, who contributes to newspapers and magazines.

- PowerShell Help
- Meaningful Content
- Real-World Exchange
- MaxTokenSize

LETTERS@WINDOWSITPRO.COM

PowerShell Help Appreciated

I want to thank Bill Stewart for his article "Auditing 32-Bit and 64-Bit Applications with PowerShell" (InstantDoc ID 136129) and the included script. After hours and hours of searching Google and learning PowerShell, I had just about given up when I happened upon the article. Thanks for making this Canuck's day!

—Karen

Meaningful Content

I'm emailing to share an IT pro's feelings about your magazine. Once a month, I walk into the mail room and I see the little corner of *Windows IT Pro* peeking out of my mail bin, and I get excited. "What cool, detailed, and accurate technical information will I find in this excellent resource?" Sadly, that feeling of excitement and anticipation has been dwindling over the past four or five months.

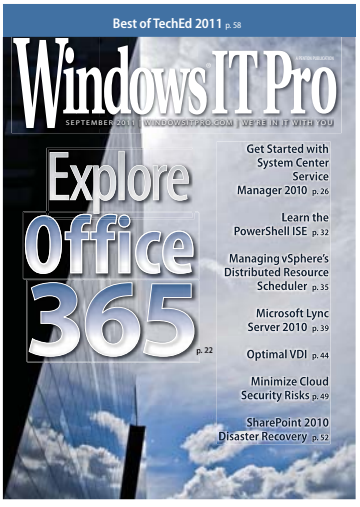
Don't get me wrong: I still love the magazine. But can you please spend less effort selling me on the cloud and get back to teaching me about servers, applications, and administrative procedures? I know the cloud is out there, and my company uses hosted applications, but no one in authority at my company is ready to house our data outside of our own purview, and we're just not interested in IT as a utility bill.

Having said that, thanks for the excellent magazine. I still look forward to getting it each month. I just hope it centers on helping professionals manage their own assets and advance their abilities and careers.

—Stoney Heflin

I hear your concerns about the cloud. When new technologies and trends emerge, we find ourselves struggling to strike a balance between educating readers on what is coming and on the technology they use today. Regarding cloud coverage, many of our readers wonder what it means for their career if more services are moved to the cloud. And they want to know what skills and technologies they need to master to stay relevant. Then again, we have many readers like you who can't or won't move to the cloud anytime soon for various reasons. It's quite a challenge to meet everyone's needs. But we'll keep trying! We appreciate the feedback and welcome other readers to share their thoughts. Drop us a line at letters@windowsitpro.com.

—Amy Eisenberg, Editor in Chief



Backup and Recovery Review

I'm looking to move away from tape backup using Symantec Backup Exec 2010. I saw Nate McAlmond's review of StorageCraft's ShadowProtect Server (InstantDoc ID 129794) and wanted to know if you had any more input between it and Symantec System Recovery Virtual Edition. My company is in the process of moving its physical servers into one virtual powerhouse and then a smaller offsite server for backing up our virtual disks for disaster recovery. I evaluated StorageCraft, and it seemed nice, but I haven't had a chance to evaluate Symantec's product. Also, do you have any opinion about Microsoft Data Protection Manager 2010?

—Rick Rosenhagen

According to its specs, System Recovery Virtual Edition looks like a comparable product to ShadowProtect Server. One major difference I see is the price. StorageCraft's product is a third the cost per server, and the company does offer a free trial. I've used Microsoft Data Protection Server in the past and liked it at first. But we ran into problems on a pretty regular basis; it failed to complete backups. Microsoft Data Protection Server does advertise the ability to back up virtual machines (VMs) from the host, whereas StorageCraft needs to be installed on each VM (unless you shut down the VMs, but this isn't supported). If I were you, I'd take a look at your Microsoft licensing and determine how much Data Protection Server is going to cost fully installed. Then decide whether it saves enough to be worth the trouble. StorageCraft was pretty trouble-free even with hundreds of gigs of data. I've been using Acronis at work for a few years now and have had good luck with that. But from what I've seen, the speed of backup and recovery with StorageCraft is quite a bit better.

—Nate McAlmond

Real-World Exchange 2010 Migration

I read, with keen interest, Brian Winstead's "Real-World Exchange 2010 Migration," (August 2011, InstantDoc IDs 136606, 136608, and 136611) about the Penton Exchange 2010 Migration. At my office, we're going through the same process. We're a much smaller organization than Penton. We have about 400 users in several locations. We've faced the same real-world budget issues as Penton, though. We aren't on subscription for Microsoft Office and are "stuck" with Outlook 2007. We'll have only two mailbox servers and will operate without a Dynamic Availability Group (DAG). Instead, we've opted to

Windows IT Pro welcomes feedback about the magazine. Send comments to letters@windowsitpro.com, and include your full name, email address, and daytime phone number. We edit all letters and replies for style, length, and clarity.

virtualize Exchange under VMware with CAS, Hub, and Mailbox roles all in one box.

One area that you didn't cover in the article is backup. I understand some organizations have multiple copies of the DAG so don't even bother to back up anymore. We have an EqualLogic SAN and are using Veeam for disk-to-disk daily backup and are doing monthly backups to transfer to tape. At some point, we hope to start replicating between two sites, but we don't have the bandwidth for that just yet.

One area where I have to differ with the Penton IT staff is regarding the importance of the new server-based archive feature. The Penton IT staff didn't see the need to bother when they can simply offer oversized mailboxes. One key point for them to consider is bandwidth. I assume most of Penton's sites will operate in Cached Exchange Mode. Let's say everyone gets a multi-gigabyte mailbox with no archive. What happens when a person sits down at a new computer? It will really strain the WAN link while it initializes the mailbox.

My approach is to set up a default archive policy that aggressively moves messages to the online archive (say, after two or three months). Outlook and OWA can still see the archive and search it, but the archive isn't part of the Exchange cache. In so doing, when a user sits down in front of a new computer, only a modest amount of mailbox data has to download. Again, thanks for the interesting article.

—Jonathan Shapiro

Thanks so much for writing! I appreciate hearing about your migration. I'd like to address your specific points about backup and personal archives. The interview originally appeared on our website in three parts, beginning with "Real-World Exchange 2010 Migration: Staging the Move" (InstantDoc ID 136608). We didn't have room for the entire interview in print. But we did talk a little bit about backup at the end of part 2 on the web. We discussed using lagged copies and moving away from tape backup. In any case, I think it was clear that Penton hoped the implementation of DAGs would be a step away from running regular backups.

Regarding personal archives, when I look at this again, I think it's kind of funny that Brent and Sean talked about the mailbox size as a reason not to use them. What we didn't talk about in this interview is our email retention policy, which is probably a bigger reason why the personal archives wouldn't be too beneficial. A couple years ago, Penton established an email retention policy based on managed folders in Exchange 2007 and Outlook 2007 such that all email is deleted after six months—unless there's a specific business case for saving it and it's moved into the appropriate managed folder. Believe me, that was a hard transition for a lot of people! The upside is that we're not maintaining the volumes of old email on the system that we otherwise would be.

Thanks again for writing. I hope your migration goes well—let me know how it turns out.

—B.K. Winstead

My Calculations Concerning MaxTokenSize

In "The Care and Feeding of the Active Directory Security Access Token" (InstantDoc ID 139827), Sean Deuby writes, "By default, MaxTokenSize is 12,000 bytes; if a user is a member of more than 120 groups, he or she might begin to experience slow logons and other erratic behavior." And then he also writes, "The MaxTokenSize value can be adjusted upward to accommodate more groups."

I think that instead of 120 groups, the number of groups mentioned should be 900, for two reasons: First, this is the number mentioned in "MaxTokenSize and Kerberos Token Bloat" at blogs.technet.com/b/shanecothran/archive/2010/07/16/maxtokensize-and-kerberos-token-bloat.aspx. Second, to adjust upward from 12,000 to 65,535 means that you increase capacity approximately by 5.5 (65,535/12,000 = 5.46125). If you have 120 groups, you increase to 120*5.5=660. Only 660 groups. This calculation does not allow us to reach the 1,015-group limit.

—Dimitrios Kalemis

Your calculations are accurate. My number of 120 groups is based on practical experience; we saw that users began to experience slow logons and occasional Kerberos-related issues beginning as low as that number of groups, though they continued to be functional to higher group levels. My text, unfortunately, makes it appear to be mathematical.

—Sean Deuby

InstantDoc ID 140714

Thinking about migrating to System z? You're in good company.

Since the start of 2010, more than 250 companies around the world have migrated workloads (including Oracle® workloads) to System z®. Why? Maybe it's the savings (up to 50% on applicable IT costs). Or the top-rated EAL5 security classification. Or because it delivers up to 99.999% availability and uptime. Or maybe it's an even better reason: all of the above.

ibm.com/facts

Thurrott

"What's unclear, currently, is whether Microsoft can wrangle the kind of reliability one expects and gets from the iPad into a traditional PC, regardless of the form factor and the variety of devices and components it utilizes."

Windows 8 and Windows Server 8 Reimagining, and Whither Windows Phone?

I've written separately and exhaustively about Windows "8" and Windows Server "8"—yes, both are still code names—but as you might expect with such major upgrades, there's a lot to discuss. So I'd like to focus on the Windows 8 and Windows Server 8 issues I didn't have time to address in my formal reviews.

Better Together?

You have to go back a decade, to Windows 2000, to find a set of Windows client and server releases that is as monumental in scope as those in the Windows 8 generation. The Win2K release, as you may recall, ushered in Active Directory (AD), DFS, disk encryption, and many other features we take for granted today. Windows 8, by comparison, offers the first major replacement of the Windows shell since 1995 and the first major replacement for the Windows runtime engine since, well, forever. Windows Server 8 overhauls how servers are managed by letting admins address multiple machines simultaneously, from a central console. And Microsoft takes major steps toward a UNIX-like future by remoting the Windows Server management interfaces, helping to ensure that fewer admins will ever have to sit in front of a server and manage it interactively.

With Win2K, and with subsequent jointly released Microsoft products, the software giant often rolled out "better together" marketing initiatives, suggesting that although either product was great on its own, only by implementing both products would you realize the true power of an integrated solution. So what about Windows 8 and Windows Server 8? Are they really "better together"?

So far, it doesn't appear so. But that might not be a negative. While Microsoft does seem to be largely ignoring the business market with Windows 8 in order to more strongly focus on consumers, I understand why Microsoft would want to make Windows 8 look and work like Windows 7 in tightly controlled corporate environments. That's because businesses that belatedly performed their migrations from Windows XP to Windows 7 aren't about to do it all again so quickly. So businesses that are looking for continuity can roll out both Windows 7 and Windows 8 and achieve a relatively consistent, training-free mixed environment.

And let's be clear here: Windows Server 8 is a huge upgrade for businesses, one that will have ramifications a decade down the road, just as Win2K does today. Therefore, staggering the big client and server changes as Microsoft appears to be doing does make some sense.

Something New

If any aspect of Windows 8 is controversial, it's the new Metro-style UI. That's understandable, as it's so different from what came before. And it appears, in this early look, to offer only super-simple, full-screen apps that couldn't possibly deliver the power and functionality of complicated "classic" Windows applications such as Microsoft Office or Adobe Photoshop.

Wrong again, everyone.

To be fair, the issue here isn't your lack of imagination, but rather Microsoft's inability to communicate not just the obvious but something that's frankly quite excellent. But that's fine, Microsoft. I can handle it for you.

Microsoft says that Windows 8 represents a "reimagining" of Windows—and, surprisingly, it does. There's a completely new runtime engine, right on top of the kernel, called WinRT that takes the syntactical elegance of .NET and supplies it with on-the-metal performance. Developers have their choice of three basic environments for writing WinRT apps—those apps that appear in the Windows 8 Start screen—including DirectX (for games) and two sets of programming languages and presentation layers. The first is JavaScript plus HTML and CSS, and the second is XAML plus your choice of high-level language (C#, Visual Basic, and more, but also C++ or even C). Those latter two environments offer identical functionality and almost identical performance.

WinRT apps share a common platform, and Microsoft provides a ton of built-in controls that developers can use to create consistent-looking applications (or not—their choice). They'll be able to sell those apps—assuming they meet Microsoft's strict compliance rules—via the new Windows Store. In fact, that's the only place where consumers will be able to get new Windows apps (as opposed to old-school "applications"), providing users with a safe, consistent platform that is, in many ways, more similar to curated smartphone platforms such as the iPhone or Windows Phone than the PC of old.

WinRT apps can take advantage of a standard set of system functions, too, including visual elements like the edge UIs—the Charms, which I'll explain in a moment—as well as a set of contracts—for intra-app sharing, like the Windows Clipboard on steroids—or file pickers that work with the local file system

and cloud storage simultaneously. Multitasking is handled by the runtime too, and as with phone apps, Windows 8 apps that aren't displayed on the screen are suspended and, should the memory be needed, automatically shut down too. (Leading to my number-one Windows 8 email query so far: How do you shut down a Metro app? Answer: You don't.) But this is OK because Windows 8 apps also can't throw up a Save dialog: Data saving is automatic, always, as is app state.

Microsoft thus far has shown off only very simple apps, but the company tells me that very complex apps are not just possible but expected. Indeed, developers can write any app for WinRT that they'd previously write for Windows. The only exceptions are NT services, device drivers—and viruses. Because WinRT apps are sandboxed from each other and from the OS, Windows 8 literally starts a new era of safer computing, one in which the bad guys are simply locked out of the system. App installs take two to three seconds, according to Microsoft, and no longer utilize the "spray your hard drive with files" approach of traditional Windows applications; instead, everything is written to a single, easily accessible (and removable) folder package. You know, like the Mac had a decade ago.

Put simply, Windows 8 is "a fire hose of new" from a platforms perspective. And by the time you read this, that fact will have begun slowly dawning on developers everywhere. It's going to be exciting.

Not bad for an OS whose version number—yes, seriously—is 6.2.

Something Old, Something New

Whether you're a PC user or an administrator of servers, it seems as if Microsoft changes interfaces with every Windows release. This has never been truer than with Windows 8 and Windows Server 8, and if you're a complainer, this is going to be a target-rich environment.

With Windows 8, it's most obvious via the new Start screen. Windows 8 also provides a new environment for full-screen apps, a new notification system, a new set of so-called Edge UIs that are available through the OS, and other new interfaces and panels that will keep OS geeks busy for months to come.

Furthermore, because the way you interact with Windows 8 differs somewhat between mouse and keyboard, touch, and pen, the ways in which you access certain UIs or features varies from mode to mode as well. Take the Charms, a set of five icons that appears on the right side of the screen when you swipe in from that screen's edge with your finger. When using a mouse and keyboard, you make the Charms appear by mousing over the lower left corner of the screen—where the Start button used to be—but not clicking. This makes a bit of sense, since users are familiar with mousing over to the old Start button location. But it's so different from how Charms are otherwise accessed that it requires you to remember both methods, since most people will use a combination of input methods.

This is just a single example, but typical of Windows 8. I've decided to just embrace it all. With great change comes new learning—we should expect this and move on.

With Windows Server 8, the user experience changes are just as vast. Yes, a Windows Server 8–based server boots into Server Manager by default as it does with its predecessors. But Server Manager is a completely different animal, an immersive Metro-style app with flat UIs, multiple panels of information, and the ability to manage multiple servers simultaneously. And as I predicted months ago, Windows Server 8 does indeed utilize the Windows 8 Start screen as well; it comes preloaded with tiles for useful management interfaces, and as you install new roles and features, tiles for those capabilities are auto-added to the Start screen too.

Performance Matters

While the Apple-friendly press and various tech pundits are trying to rewrite history as it happens by obfuscating the relative success of the iPad with the relatively slow growth of the PC market, the numbers are simple: At its most successful, the market for iPads and iPad-like tablets will be one-tenth the size of the still-growing PC market this year. At best.

But the iPad does bring some useful capabilities to market, not the least of which are the device's performance. Say what you will about the Fisher Price–like qualities of the iPad, but the thing is fast.

If the Developer Preview is any indication, Windows 8 is going to be bringing iPad-like performance to the PC market. I've seen boot times of five to eight seconds on all of my own PCs. I've seen Windows 8 wipe out the entire install, reinstall Windows, then reapply all of my custom settings, documents, and Metro-style apps—in just five minutes.

Windows 8 (and Windows Server 8) also employs some cute tricks to bolster overall performance in small but meaningful ways. Take Windows Update, please. Windows 8 will download updates in the background and intelligently install those that don't require reboots first.

What's unclear, currently, is whether Microsoft can wrangle the kind of reliability one expects and gets from the iPad into a traditional PC, regardless of the form factor and the variety of devices and components it utilizes. The Developer Preview build we have now is far too early—and far too buggy—for an accurate assessment. But it's something I'll be monitoring going forward. Normally I wouldn't even dream this big. But the performance picture is so solid, I'm starting to wonder.

Whither Phone?

Microsoft hasn't publicly admitted this yet, but I've heard from multiple sources that the next major release of Windows Phone, which could hit as early as Q3 2012, will indeed be based on Windows 8, providing Microsoft's smartphone platform with modern underpinnings, a consist user experience, and, most intriguingly, app compatibility with the desktop. Is this going to happen? I think so, and if it does, Windows Phone could experience a surge in popularity thanks to the superior Metro-style UI. Which means that predictions about a sudden rise in Windows Phone's fortunes were based on more than just wishful thinking.

InstantDoc ID 140718

PAUL THURROTT (paul@windowsitpro.com) is the senior technical analyst for *Windows IT Pro*. He writes the SuperSite for Windows (winsupersite.com), a weekly editorial for *Windows IT Pro UPDATE* (www.windowsitpro.com/email), and a daily Windows news and information newsletter called *WinInfo Daily UPDATE* (www.wininformant.com).

Minasi

"Here's a situation where PowerShell remoting can help out."

Go Remote with Windows Server 2008 R2's AD Cmdlets

You're sitting at a Windows 7 workstation and need to perform a query against AD—What do you do?

Last month, in "Find Users with Get-ADUser" (InstantDoc ID 140069), I showed you how to use Windows Server 2008 R2's new Active Directory (AD)-related PowerShell cmdlets to perform AD maintenance tasks quickly and consistently. Using AD's PowerShell cmdlets can get a little irritating, however, as not every Server 2008 R2 or Windows 7 system has the AD module on it. (Remember, you can issue R2's AD cmdlets from only those two OSs.) Of course, you could just download the Remote Server Administration Tools (RSAT) to get that module, but that would probably take more time than just going back to the office. That's where PowerShell remoting helps out.

Suppose you're sitting at a Windows 7 workstation and need to do a *get-aduser* query like last month's. If you know the name of a Server 2008 R2-based DC (let's call it DC64), you might be able to enter these four commands right at your Windows 7 box:

```
enter-pssession dc64
ipmo ac*
get-aduser -f {givenname -eq 'Mark'}
exit-pssession
```

Those two new commands—*enter/exit-pssession* (or *etsn/exsn* for short)—enable PowerShell remote control atop the Windows Remote Management (WinRM) protocol that's existed in Windows since Windows Vista, and they're great because the Windows 7 system needs no previous setup to make this work.

The target of those commands, however—DC64—does need a bit of prep work before it can be remotely controlled. First, its firewall needs to be either in Domain or Private mode and, second, it needs something called a *WinRM listener* enabled. Out of the box, Windows computers can initiate WinRM sessions but can't "hear" other systems ask them to participate in WinRM sessions unless you enable those computers' WinRM listeners by typing this command from an elevated command prompt on those computers:

```
winrm quickconfig -q
```

If you prefer to use Group Policy to enable listeners on many systems en masse, enable the setting *Allow automatic configuration of listeners* in Computer Configuration, Administrative Templates, Windows Components, Windows Remote Management (WinRM), WinRM Service. If you decide to create a Group Policy to enable remote sessions, remember that in general you need enable it only on the servers. (DC64 needs the listener; your Windows 7 box doesn't.) Alternatively, PowerShell has a way to enable or disable WinRM listeners in its *enable-psremoting* and *disable-psremoting* cmdlets.

Besides *enable/exit-pssession*, you can similarly send one or more PowerShell commands to a remote system using another PowerShell cmdlet, *invoke-command* or *icm*. Its syntax looks like

```
invoke-command computer-to-run-command-on { command ;
  command ; command…}
```

You need to enter two commands (the *ipmo* and the *get-aduser*), so your *invoke-command* cmdlet will look like

```
icm dc64 {ipmo ac* ; get-aduser -f {givenname -eq 'Mark'}}
```

Notice a few things here. First, the PowerShell term for the thing between the curly braces is a *script block*, which really just means "one or more cmdlets." The script block is two commands separated by a semicolon—the *ipmo* and the *get-aduser* commands. Notice that the smaller command inside that script block (*givenname -eq 'Mark'*) isn't a script block; the PowerShell folks decided to use braces to store query/filter criteria early on, so the folks on the Directory Services team apparently decided to use them for *get-aduser*'s filter parameter. It's a bit confusing, but just remember that in PowerShell, in general, you'll only see braces used to designate one or more cmdlets that work together—a script block—or to surround some logical criterion.

Second, let me clarify something about PowerShell grammar. Searching for "invoke-command" on the Internet will yield a zillion examples that look like

```
invoke-command -computername dc64...
```

but notice that my command lacks *-computername*. I've left that out because although PowerShell tends to require explicit parameters and operators like *-computername, -filter,* and *-eq* rather than positional parameters, it bends that rule when there's a commonly used parameter, as is the case with *-computername*. It's all a matter of taste, but I like my PowerShell commands to be as short as is possible. Next month, more queries!

InstantDoc ID 140491

MARK MINASI (www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 30 books.

Otey

"If you get the hang of using Jump Lists, you'll probably find you want to display more than the default 10 items."

Windows 7 Productivity Tips

Get max efficiency from libraries, Jump Lists, the Windows Explorer, and other features

Windows 7 has been out for a while, and by all accounts has found its way into many people's daily working lives. However, it's easy to just keep doing things the old way instead of learning about new features that can help you work more efficiently. Here are 10 handy Windows 7 productivity features that you might have overlooked.

10 **Take advantage of libraries—**Windows 7 libraries help you better organize the files and folders on your hard disks. Unlike folders, libraries don't actually contain any files; they contain only pointers to file locations. To make a new library, open Windows Explorer, right-click the Libraries node in the left pane, and select New, Library. To point the library to existing folders, right-click the library, select Properties, then click *Include a folder*.

9 **Quickly open recent documents using Jump Lists—**Jump Lists are super handy when you run a lot of applications because they let you quickly bring up recent documents. To open a Jump List, right-click a program icon in the taskbar. Alternatively, you can use the Start menu and click the arrow to the right of each program name.

8 **Display more items on your Jump List—**If you get the hang of using Jump Lists, you'll probably find you want to display more than the default 10 items. To customize your Jump Lists, right-click the taskbar, click Properties, then select the Start Menu tab. Click the Customize button. At the bottom of the Customize Start Menu dialog box, you can adjust the number of items displayed by your Jump Lists.

7 **Open a command prompt from Windows Explorer—**Jumping into a command prompt from the current folder you're displaying in Windows Explorer is easier in Windows 7 than it was in any previous version. Hold down the Shift key, right click the folder name displayed in the left column of Windows Explorer, then select the *Open command window here* option.

6 **Launch programs with elevated rights—**In still too many instances, you need to run programs with administrative rights. To run a program from the Start menu with elevated rights, open the Start menu, then right-click the program icon and select *Run as administrator*. It's not so obvious, but you can also launch Windows Explorer and taskbar programs with elevated rights by pressing Ctrl + Shift, then clicking the program.

5 **Dictate speech using Windows Speech Recognition—**Windows has the built-in ability to perform voice recognition for commands and dictation. To use Windows 7 voice recognition, click Start, All Programs, Accessories, Ease of Access, and select Windows Speech Recognition. After Windows Speech Recognition starts, you can click the microphone button to start voice commands. Ironically for an Ease of Access item, this is pretty difficult to use and the tutorial is a must.

4 **Print from Windows Explorer—**Another timesaving tip is the ability to print directly from Windows Explorer without first opening the target program. For instance, if you want to print a Word document or Excel spreadsheet, just navigate to the item in Windows Explorer, right-click it, and select Print from the context menu. The document will be printed on your default printer.

3 **Post reminders with Sticky Notes—**Tired of all those yellow Post-it notes everywhere around your monitor? You can use Windows 7 Sticky Notes to move them all to your computer desktop where you can organize them and page through them. Different notes can have different colors and fonts. To use Sticky Notes, click Start, All Programs, Accessories, Sticky Notes. Move the note where you want it and just type into it.

2 **Pin programs to the Start menu—**I probably use this too much, but the Start menu is a super handy place from which to launch frequently used programs without cluttering up your desktop. To pin a program to the Start menu, click All Programs and locate a frequently used program. Right-click the program and select Pin to Start Menu from the context menu.

1 **Use MSConfig to clean up your startup programs—**The inevitable curse of Windows is that, after you run it for a while, it becomes all junked up with all kinds of extraneous and unwanted programs—many of these running automatically every time your system starts. To clean up your startup items with MSConfig, go to the Start menu and enter *msconfig* in the search box. Select the Startup tab, then clear the check box for the programs you don't want to start automatically.

InstantDoc ID 140557

MICHAEL OTEY (motey@windowsitpro.com) is senior technical director for *Windows IT Pro* and *SQL Server Magazine* and author of *Microsoft SQL Server 2008 High Availability with Clustering & Database Mirroring* (McGraw-Hill).

Deuby

"Determine whether there are any major road blocks to deploying Office 365."

Is Your Identity and Access Infrastructure Ready for the Cloud?

The Office 365 Deployment Readiness Tool will give you a reality check

Most of the talk about cloud security and cloud identity has been directed at the cloud service provider and applications, and the various methods your company can use to provide single sign-on (SSO) and identity security working with these apps. At the same time, we shouldn't neglect the state of our own identity and access management (IAM) infrastructure. Is it ready to handle the new requirements and challenges that federation and cloud services will put on it? Fortunately, there's a free tool available to help you assess this.

Preparing your identity and access infrastructure to interact with web services via federation is a topic worthy of exploring in some detail, which I'll be doing in an upcoming article. In this column, I want to focus on a utility Microsoft developed to make migration to its Office 365 SaaS suite easier. The Microsoft Office 365 Deployment Readiness Tool (a name apparently untouched by anyone in Marketing)—currently in beta—does exactly what the name says: It analyzes different aspects of your current environment to determine if there are any major road blocks to deploying Office 365.

What the Tool Does

Whether or not you're planning to use Office 365, don't stop reading! Everyone with an Active Directory (AD) forest should run this tool as a free, quick, and easy way to check the consistency of his or her AD data. It's also a great tool for system integrators to run a quick check on a customer's AD environment to quickly gauge the complexity of what they're getting into.

The Office 365 Deployment Readiness Tool makes assessments in seven sections: Domains, User Identity and Account Provisioning, Exchange Online, Lync Online, SharePoint Online, Client and End User Experience, and Network. Which assessments you care about depends on which, if any, Office 365 components you're planning to deploy. If you're just looking to run the tool against your forest to see what errors it flags, you'll care about the Domains and User Identity and Account Provisioning assessments. Because this is a column about enterprise identity, we'll focus on these assessments.

Designed by former Microsoft Consulting Services engineers, the tool performs a comprehensive suite of tests against your AD and SSO environment. One of the main purposes of the AD-related assessments is to check how well your AD implementation would work with Office 365's Directory Synchronization Tool. DirSync is a critical Office 365 component, running on a dedicated server in your environment, that integrates your on-premises directory information—users, groups, and contacts—with the Office 365 infrastructure in the cloud. With DirSync, you make all changes to your users, groups, and contacts in your own AD environment, and the updates are synchronized with the Office 365 cloud. DirSync is also necessary to provide an SSO experience for your users.

The first questions you should ask about this tool are, "How intrusive is it?" and "Does it require any administrative rights?" The answer to the first question is: No, it's not intrusive. It's been tested with customers who have very large AD installations of more than 300 users, so it scales to large environments without interfering with daily operations. The answer to the second question is: No…ish. Read on for more detail.

Running the tool is simple; in fact, it's disconcertingly simple. When you unzip and run office365deploymentreadinesstool.exe, you expect the Welcome screen of the tool's installation wizard. But there's no welcome screen: The tool has already begun analyzing your environment. (It feels vaguely like malware.)

What the Report Shows

When the tool has finished running, it generates a long browser page containing all the assessment results, separated by sections, with a link for the online version of the complete enterprise deployment guide. A nice touch is that there's a link at the top of each section that takes you to the appropriate section of the online deployment guide. This makes it easy to get guidance when you get results you need to follow up on. The page is stored at C:\office 365reskit\htm\assessmentrunning.htm—good to know if you accidentally close the browser window.

The first action you'll want to take is to click the CSV File Maker link. Doing so will extract and prompt you to save a utility to create .CSV files of exceptions generated by the reports. Save it, and run it, and it will create all the .CSV files you need to examine. If you should happen to click a *Review the Results* link before you've run CSV File Maker, the link will tell you to run it first.

Domains. The Domains section simply lists the number of email domains and primary email domains (reply-to addresses) that the tool discovered.

User Identity and Account Provisioning. The User Identity and Account Provisioning section delves into the security principals in your AD environment. It has four subsections that review different aspects of your identity infrastructure. It also displays some interesting statistics that are often hard to come by and might, by itself, make running the tool worthwhile. It displays the total number of domains in your forest—which you hopefully already know!—but also the number of your users, contacts, groups, and mailboxes across the entire forest. It also displays the total number of objects that will be used by DirSync. Note that this is *not* the total number of objects in your AD forest; this count doesn't, for example, include computer objects, which outnumber users in a typical forest.

Forest and Domains. The Forest and Domains subsection provides information about the active and inactive trusts associated with your forest, and what kind of trusts they are: unidirectional, bidirectional, down-level (e.g., NTLM) or up-level forest trust, and whether the trust is transitive. In my case, it reminded me of an old trust I'd set up with a test forest named sandbox .test. If the tool does discover a forest trust, it will generate a warning that DirSync supports only one logon forest—that is, a forest containing user accounts. Though we'd all like to have one master account directory (even if it's a metadirectory or virtual directory), for various legitimate business and regulatory reasons many companies have separate account forests. Office 365 doesn't currently support more than one account forest, but I'm confident this large-enterprise restriction will be lifted soon. The initial DirSync capabilities had to cover most companies' configurations, but releasing products directly to web (RTW) ensures that new features can be rolled out rapidly, and I'm sure a multi-forest sync capability is a high priority.

Schema and Forest/Domain Functionality Levels. The Schema and Forest/Domain Functionality Levels subsection displays the forest schema level, the Exchange schema level, and the domain and forest functionality levels. If your schema has been upgraded to handle Exchange Server 2010 SP1 or later, the tool will display a warning that the schema isn't ready for an Exchange Hybrid Deployment (in which some mailboxes are on premises and others are in Exchange Online).

Active Directory Cleanup. The Active Directory Cleanup subsection is where you'll probably find the most value in this tool. It inspects a few key AD attributes across your forest for inconsistencies that will cause an Office 365 migration to generate errors or fail. Whether or not you deploy Office 365, you should clean up data inconsistencies in your forest; sooner or later, these inconsistencies will trip up future AD-integrated applications that require AD data, or enhancements to your identity infrastructure such as a metadirectory or virtual directory.

This section checks sAMAccountname (user name), gIVENName (first name), sN (last name, aka surname), and dISPLAYName for character length and unsupported characters. It also checks mail (email address), mAILNickname, and pROXYAddresses for spaces and duplicates. Unfortunately, it doesn't check for consistency in phone numbers or other attributes you might think are useful, because Office 365 doesn't require this. If you do have errors in this section, or any other section that requires attention, the tool will display a link to a .CSV formatted file with the data in error so that you can attack the errors programmatically.

> The free Office 365 Deployment Readiness Tool gives you a quick assessment of your AD, Exchange, and SharePoint environment.

Directory Synchronization. The Directory Synchronization subsection provides an assessment of the number of objects DirSync will run against (and therefore be uploaded to Office 365). Interestingly, if the object count is greater than 10,000, you'll be prompted to contact Office 365 support to notify them how many objects you need to upload. This is to prevent Denial of Service (DoS) attacks. Note that some of these "more information"-type links open in new tabs and some don't, so pay attention when you follow the links so that you don't accidentally close the assessment report.

This section also does an Enterprise Admin check. "An EA check?" you ask. "Doesn't this tool run without elevated privileges?" Yes, it does; this check is for privileges needed to install DirSync—not the Readiness Tool; during the DirSync installation, you're asked to provide EA credentials. Why does DirSync need EA privileges to install? From the documentation: "The (DirSync) configuration wizard uses Enterprise Admin credentials to create the directory synchronization service account, MSOL_AD_Sync. This service account is created as a domain account with directory replication permissions on your local Active Directory and with a randomly generated complex password that never expires…these credentials are erased from the computer's memory after the service account is created." This section also performs a check for user principal name (UPN) duplicates and that every user is assigned a UPN; this will affect your ability to implement SSO with Office 365.

The tool also performs a basic Exchange assessment, listing the Exchange servers in the environment, users, and public folders. It also runs network tests to ensure that your network can reach Office 365.

A Great Start

The Office 365 Deployment Readiness Tool is a free, easy-to-use utility that gives you a quick assessment of your AD, Exchange, and SharePoint environment. It's not comprehensive, but it's a great way to give you an idea of how much cleanup work must be done before you begin extending your identity information beyond your company's borders. The Microsoft Office 365 Deployment Readiness Tool is available at http://bit.ly/qhrJRL.

InstantDoc ID 140661

SEAN DEUBY (sean@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Magazine*, and former technical lead of Intel's core directory services team. He's been a directory services MVP since 2004.

READER TO READER

Avoid Browser Hijack Viruses

I recently watched a local TV news report about the latest crop of browser hijack viruses, which are disguised as anti-virus programs. For example, in the "Antivirus 2009" attack (Figure 1), a security alert pops up telling you that it's running a scan, after which it gives you the bad news that your computer is infected with viruses and other malware. Figure 2 shows a more generic "Message from web page" attack, which notifies you that there are signs of viruses and malware on your computer. Some of these disguised programs try to get you to purchase a program that will remove the malware, whereas others tell you that you can download a free removal program. Either way, if you try to download the program, your machine will become infected with a single click. (To see the TV news report about the browser hijack viruses, go to www.wptv.com/dpp/money/consumer/dont_waste_your_money/'disguised'-computer-virus-.)

Bret Bennett

To thwart these attacks, the report advises you to "close out the web browser immediately." Anyone who has experienced this type of attack knows you can't close the browser by any *normal* means. The only apparent exit strategy is to click something on the hijacked screen, such as a Cancel, Exit, or No Thanks button. When clicked, the machine becomes infected.

There are countless anti-malware products and how-to articles on the web that provide complicated disinfection procedures. However, there are two best-practice lines of defense, as well as other solutions, including one easy procedure that I use.

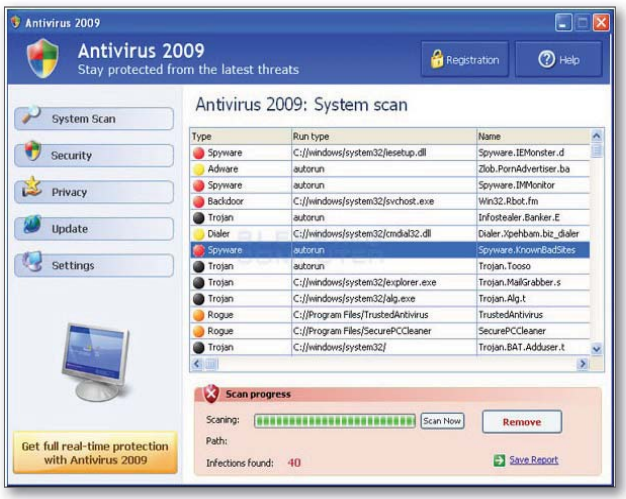


Figure 1: "Antivirus 2009" attack

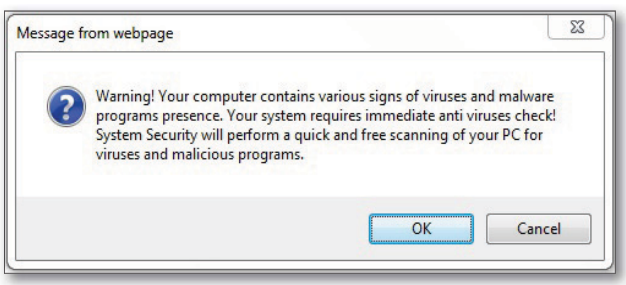


Figure 2: Generic "Message from web page" attack

On newer Windows OSs (e.g., Windows 7, Windows Vista), one best practice is to keep User Account Control (UAC) enabled. When it's enabled, an attack program will trigger a UAC prompt because the program is trying to perform an operation that requires Administrator-level permissions. The user must be savvy enough to click No when presented with the UAC dialog box.

The other best practice is to not set the user account type to Administrator—although some legacy line of business (LOB) software won't run unless the user has administrative privileges. Similarly, some nonlegacy utilities require administrative privileges.

In addition to these two best practices, there are other safe-browsing solutions, including antivirus software that lets you browse in "sandbox" sessions. (In these sessions, you lose OS functionality such as cut and paste.) Alternatively, you can do your browsing on a virtual machine (VM) that's isolated from the Windows OS.

I use a technique that doesn't require additional software and lets you keep the user account type set to Administrator. Suppose you receive a warning message like that in Figure 2 on a computer running Windows 7. First, *don't click anything in the open browser window or open a new browser session.* Instead, follow these steps:

1. Check the program icons in the taskbar (or tap Tab while holding down Alt) to see if additional bogus dialog boxes or forms are being spawned by the initial unwanted browser hijack program. Figure 3 shows an additional Windows form that was an offspring of the "Message from web page" attack. You can't see this form running on the main screen because it's hidden under the *Message from webpage* dialog box.
2. Click Ctrl+Alt+Delete to bring up Windows Task Manager.
3. On the Applications tab, find the Internet Explorer (IE) application that reflects the URL you can see in the infected IE window's address bar. Right-click the offending

Tell the IT community about the free tools you use, your solutions to problems, or the discoveries you've made. Email your contributions to r2r@windowsitpro.com.

If we print your submission, you'll get $100.

Submissions and listings are available online at www.windowsitpro.com. Enter the InstantDoc ID in the Search box.

IE application and select Go To Process. You'll be taken directly to the instance of IE that's under attack in the Processes tab.

4. Click the End Process button.

It's that easy. The attack has been defeated—well, maybe. This particular attack still had some life in it after I clicked the End Process button. If this happens to you, you need to repeat steps 2 through 4. You'll know when you're victorious when you receive a message like that in Figure 4.

At this point, you'll still see the remnants of the defeated attack in the *Website restore error* tab, as Figure 5 shows. You can close the tab because you've safely avoided the virus. Note that when the attack occurred, I had several other IE instances running in the same browser session. During this entire defensive maneuver, I never closed a single one, as you can see in Figure 5.

Out of curiosity, I tried to induce another "Message from web page" attack. I opened a new IE session and typed in the base domain with the "www." prefix. This time my antivirus product intercepted the attack. As this demonstrates, there's no single antivirus product that catches all malware all the time. In this instance, I'm guessing that the antivirus product was able to detect the threat potential for one of the following reasons:

- It originated from a fresh IE session in a fresh IE instance (unlike the first attack, which originated from a search engine link).
- The browser redirect had been corrected by the search engine.
- The antivirus product had been updated since the original attack.

To verify that nothing crawled through during the original attack or during my attempt to intentionally induce the attack, I scanned the Temporary Internet Files folder. I also made sure that no strange services were running in Task Manager. In Services .msc, I once saw a service named something like XYZWW6CY after an attack on a PC. The service wasn't started, but with a random name like that, I suspected it was up to no good and did some investigating. I ended up deleting its entry in the HKLM\SYSTEM\CurrentControlSet\services registry key.

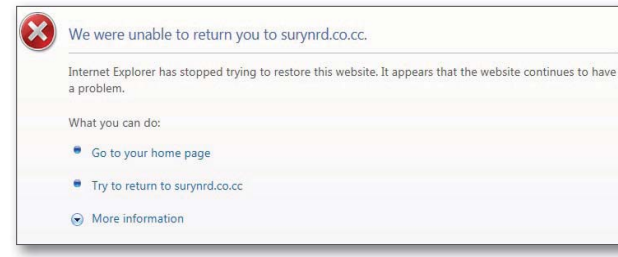


Figure 4: Message indicating that the attack has been defeated

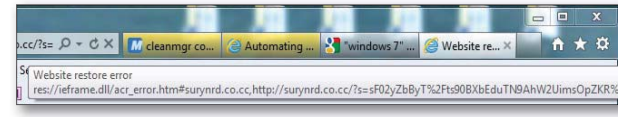


Figure 5: Remnants of the defeated attack in the *Website restore error* tab

While in Task Manager, I also rechecked the Processes tab. Plus, I ran the System Configuration Utility (msconfig.exe) and checked the utility's Services and Startup tabs for unusual listings. Finally, I performed a quick scan with my antivirus program. I didn't find anything suspicious during these checks, so I felt confident that the attack had been thwarted.

—Bret Bennett, IT consultant

InstantDoc ID 140563

Set Up Meaningful Text Messages

Apostolos Fotakelis

I recently faced a situation where some attachments were being removed from incoming emails for no obvious reason. Instead of the attachment, all the user was getting was a text file that, when opened, read "This attachment was removed." This was anything but useful, as it didn't help identify at which part of the email route the attachment was being removed. It could have been removed at the sender's end or the receiver's end. And at each end, there are many different components involved, such as the local computer's antivirus program, the mail server's antivirus program, the mail server itself, the demilitarized zone (DMZ) firewall, the inside firewall, or even the intrusion prevention system (IPS).

To test the internal Microsoft Exchange Server mail system, I sent an email to another internal user with the same type of attachment. This test revealed that it wasn't something internal that was removing the attachment. This made things more complicated, especially since the original email composer (an external user) could send the attachment successfully to other recipients. Then it hit me: The link between the internal and external email systems is the DMZ, which pointed to the Edge Transport server.

The Get-AttachmentFilterEntry and Get-AttachmentFilterListConfig cmdlets, which are part of the Exchange Management Shell (EMS) cmdlets, revealed the root of the problem. Apparently, Exchange was set up to remove this type of attachment, but by default, it put in the generic "This attachment was removed" text message. So, I used the following command to change the text file's message to one that would be more helpful in future troubleshooting efforts:

```
Set-AttachmentFilterListConfig
  -Action Strip -AdminMessage
  "Edge Transport server on site X
  has removed this type of content"
```

(Although this command wraps here, it should be entered all on one line.)

The moral of the story is that to make troubleshooting much easier, you should configure your security software (e.g., antivirus programs, firewalls) to provide you with enough information to point you in the right direction. Replace the default messages with messages that are meaningful and unique to your organization.

—Apostolos Fotakelis, computer security engineer, MCT

InstantDoc ID 140564

Figure 3: Offspring of the "Message from web page" attack

Paul Thurrott...

. . . he's not in Microsoft's pocket, but now he can be in yours.

The independent voice for IT enthusiasts

Paul Thurrott delivers news, tips, commentaries, and reviews on Microsoft technology – from gaming to mobile to servers to software, and coverage of Microsoft competitors in between. Get daily updates without reaching farther than your pocket.

Download your
Paul Thurrott: PocketTech app today

windowsitpro.com/mobile-apps

Available for iPhone | Windows Phone 7 | Android

- Personal Folders
- Key Management Services
- Xbox 360
- BitLocker
- Hyper-V
- Windows Thin PC

ANSWERS TO YOUR QUESTIONS

Q: Is there a way users can easily back up their own PSTs?

A: Microsoft has an add-in utility to let individual users back up their Personal Folders (i.e., .pst files) from within Microsoft Outlook. The tool, Pfbackup, was originally intended for Outlook 2003 and Outlook 2002, but it works fine with Outlook 2007, and with some configuration, it can work with Outlook 2010 as well.

The add-in is a small, 160KB download with a simple installation. You can download the utility from the Microsoft Download Center: Personal Folders Backup. You can install the add-in with Outlook running, but you'll need to restart Outlook to load the new utility.

If you didn't already have an add-in installed for Outlook 2010, you'll now have a new tab on your Outlook Ribbon called Add-Ins. Other Microsoft add-ins will create this tab as well, such as the Bing Travel Add-In for Outlook (see "Q: How Do I Install and Use the Bing Travel Add-In for Outlook 2010?" InstantDoc ID 126083). Pfbackup didn't create a nice icon for the Ribbon in my tests, but the word Backup on the Ribbon is itself the button. Launching the Pfbackup add-in opens a simple interface. Clicking Options opens the configuration window.

You can set Pfbackup to back up multiple .pst files, and you can control the location of the backups through the interface. For Outlook 2010 on Windows 7, by default, backups reside in \Users\<username>\Documents\Outlook Files. You can back up .pst files with a quality, uninterrupted connection to a remote network location. You can configure Pfbackup to remind you to back up your .pst files after a certain number of days, ranging from 1 to 60. If you enter a number greater than 60, the add-in uses the maximum reminder interval of 60 days. The default reminder interval is 7 days.

After the accounts for backup are selected and their backup destinations assigned, click OK on the Backup Options window and the Save Backup button to set Pfbackup. You'll then see a dialog box that states that the backup is performed when you exit Outlook.

It's important that you don't shut down your workstation immediately after exiting Outlook if you have a backup operation configured. Pfbackup doesn't provide a comprehensive interface identifying the progress of its operation. It doesn't show anything at all indicating that the backup has even started or finished. If you have a large .pst file to back up, leave the workstation on long enough to allow that file to be copied. For instance, a 2GB .pst file might take 15 minutes to backup. The efficiency of Pfbackup depends on workstation performance, especially disk I/O operations, because Pfbackup is for the most part a file copy service.

There are a few catches to using Pfbackup in Outlook 2010. First, Pfbackup is a 32-bit add-in and won't work with 64-bit Outlook 2010. Second, Pfbackup copies Personal Folders immediately after Outlook is shut down. Microsoft has made changes in Outlook in response to user feedback that allow Outlook to close more efficiently; as a result, in Outlook 2010 the Pfbackup add-in doesn't automatically execute as with previous versions. A registry entry is required for Pfbackup to initiate when the user exits Outlook 2010. A value of 1 needs to be assigned to a new DWORD entry named RequireShutdownNotification at HKEY_CURRENT_USER\Software\Microsoft\Office\Outlook\Addins\Microsoft.OutlookBackup.

—William Lefkovics

InstantDoc ID 139916

Q: I have several programs set to launch via the RunOnce registry keys, but they're not starting when a user logs in. Why not?

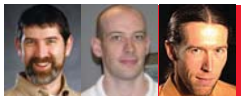
A: There are several registry keys that allow an application to launch once, normally for some kind of initial setup process:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunonceEx

These keys are frequently used by malware. To increase security, commands set to execute in these keys don't run when a normal user logs on—only when an administrator logs on, per the Microsoft "Standard user: RunOnce and RunOnceEx are not being executed" (see support.microsoft.com/kb/2021405). If you want a process to run for a normal user, consider using a scheduled task.

—John Savill

InstantDoc ID 139921



William Lefkovics | william@mojavemediagroup.com
John Savill | jsavill@windowsitpro.com
Greg Shields | virtualgreg@concentratedtech.com

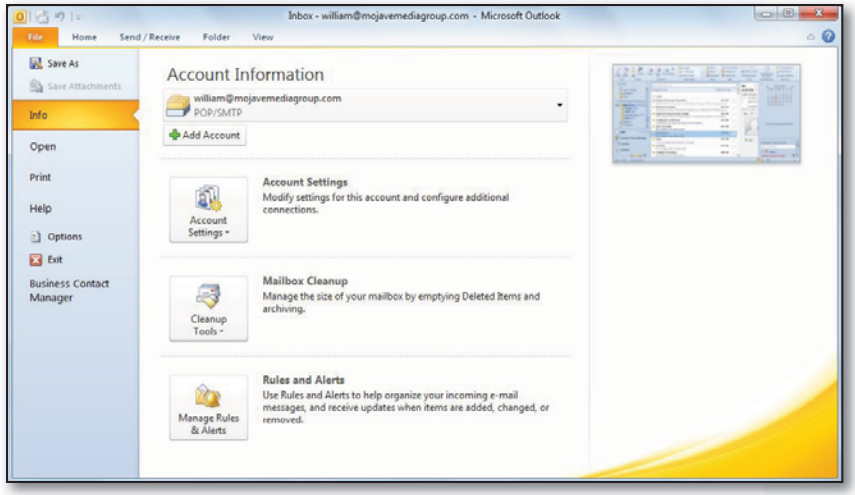


Figure 1: The Backstage view for the main Outlook window

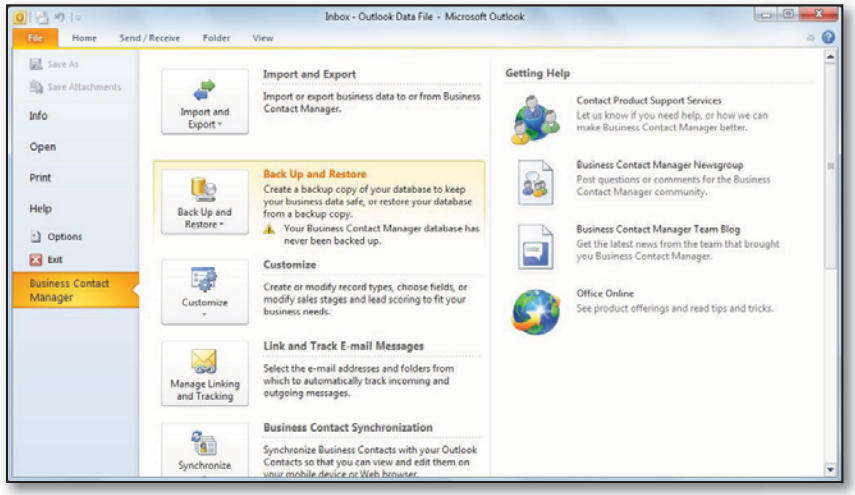


Figure 2: Configuration options for BCM in the Outlook Backstage view

Q: What is the Outlook 2010 Backstage view?

A: The User Experience Team for Microsoft Office 2010 made some changes to the Office Ribbon that significantly affect Microsoft Outlook. First, Outlook was one of the last applications in the Office suite to fully adopt the Ribbon across all standard Outlook forms. (For information about Outlook forms, see "What is an Outlook form?" at www.windowsitpro.com/article/outlook/outlook-form-136198.) But the biggest change was probably the addition of the Office Backstage view.

Microsoft separated tasks completed within the application (e.g., changing the Inbox view in Outlook, switching fonts in a new email message) from tasks you need to perform outside the application (e.g., adding accounts, configuring archiving). Many of these outside tasks were traditionally located in Tools, Options or Tools, Accounts. They're now located in the Backstage view, which is accessed using the File tab at the top left of the Outlook Ribbon. Figure 1 shows the Backstage view for the main Outlook window. It looks similar to the Backstage view of other applications in the Office 2010 suite.

The Backstage view holds configuration options and settings you would access outside of a specific email message or other Outlook form (e.g., task, appointment) you're working on. The Options button in the left pane opens a window similar to the Options dialog box in Outlook 2007 and earlier.

The options available in the Backstage view are slightly different depending on where you were in Outlook when you accessed it. If you access the Backstage view from the File tab in a new email message, the options include things you might want to do with the message itself, apart from manipulating the content of the message. These options include moving folders, setting permissions, or saving the message as an .msg file. Add-ons can also leverage the Backstage view. For example, if the Outlook Business Contact Manager (BCM) is installed, it will be visible in the navigation pane on the left of the Backstage view, and configuration options for BCM are available there, including database backup options, which Figure 2 shows.

Moving configuration options to the Backstage view has helped keep the Outlook Ribbon options simpler and focused on the work you're doing, and hopefully that keeps you more efficient.

—William Lefkovics

InstantDoc ID 139886

Q: What services does vShield Edge provide?

A: Networks have special requirements when their configuration goes beyond the traditional LAN, such as DMZs and VPN extranets. They can also be the networks that extend internal services into the cloud. Being different than a typical LAN, their connections must be secured, firewalled, and properly routed to ensure network protection. Managing these services "at the edge" of the network is a common tactic.

vShield Edge provides a suite of common gateway services that support such security requirements. Its services include firewall protection with network ACLs, DHCP, VPNs, NAT, and load balancing. Linked directly into the vSphere environment, vShield Edge applies these rules on vCenter port groups, vNetwork Distributed Switch port groups, and the Cisco Nexus 1000V.

If you're considering extending your LAN into the public cloud for Hybrid Cloud Computing, vShield Edge's gateway services are designed to ensure VMs hosted elsewhere can securely connect back into your LAN.

—Greg Shields

InstantDoc ID 139897

Q: Is there a hard limit to the number of users that can be logged on to a single Windows 7 workstation using Fast User Switching?

A: It's possible for multiple users to be logged on to a single Windows 7 instance through the fast user switching feature, which lets a new person log on without logging off the current user. The previous user session runs in the background. Only one logon can be active at any time, but the other user sessions are all still running in the background.

There's no hard limit to the number of users that can be logged on through fast user switching, only the resource constraints of the machine. Every logon will consume a certain amount of resources, so eventually the machine will run out. If the users who're logged on have applications running when their sessions are switched, they'll consume more resources.

—John Savill

InstantDoc ID 139915

Q: How can I check if I have Office 2010 SP1 installed?

A: When you install Office 2010 SP1, the Help information might not obviously show the service pack is installed. If you click *Additional Version and Copyright Information*, you can see detailed information, including the service pack version. You can also tell by the build numbers:

- Office 2010 RTM - 14.0.4760.1000
- Office 2010 SP1 - 14.0.6023.1000

—John Savill

InstantDoc ID 139917

Q: I want to set up multiple Key Management Services (KMS) in my environment. Can I use the same KMS key on all of them?

A: Many organizations opt to use a KMS internally, which is fairly easy to install. You set up a KMS key and clients, then activate with the internal KMS server instead of Microsoft. This is used only for the initial activation—clients need to check in every 180 days, and they'll actually try and reactivate every seven days, which then resets the 180 day counter. (So even if the KMS server is unavailable for a while, it's unlikely you'll have problems with your clients, because they should have plenty of time left on their activations.) If your KMS server fails, it's very easy to stand up a new KMS server in its place.

You might still want multiple KMS servers, either for geographic distribution (which is the most common reason), or simple scalability. The KMS key you receive can be used on up to six KMS servers in your organization, per these Microsoft FAQs (www.microsoft.com/licensing/existing-customers/product-activation-faq.aspx). However, if you contact the Microsoft activation center, they can enable additional activations for your KMS key.

—John Savill

InstantDoc ID 139918

Q: How can I let non-administrators perform activation actions on a client?

A: To let normal users perform activation actions, such as changing Multiple Activation or Key Management Service keys, performing a re-arm, or installing a license, do the following on the client:

1. Start the registry editor (regedit.exe).
2. Move to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform.
3. If the DWORD value UserOperations doesn't exist, create it.
4. Double-click UserOperations and set it to 1. Click OK.
5. Close the registry editor and reboot the client.

—John Savill

InstantDoc ID 139919

Q: What version of Internet Explorer (IE) does Windows Thin PC include?

A: Windows Thin PC is based on Windows Embedded Standard 7. It's for machines that primarily act as thin clients—it supports RDP 7.1. Thin PC includes IE 8. You can install IE 9 by going to this Microsoft site, but IE9 isn't available on Thin PC via Windows Update.

—John Savill

InstantDoc ID 139920

Q: I notice that different guest OSs have different numbers of virtual processors supported with Hyper-V. What happens if you try to assign more than the supported number of virtual processors?

A: Hyper-V in Windows Server 2008 R2 supports up to four virtual processors per virtual machine (VM), but different guest OSs running within those VMs are tested with different numbers of processors—not all guest OSs are supported for use with the full four virtual processors. The full list of OSs and supported number of virtual processors can be found on this Microsoft site.

If you install a guest OS that, for example, is listed as supporting only two virtual processors, but you configure the VM with four virtual processors, it will still boot—there's no hard limit. However, the configuration wouldn't be supported, and there might be valid performance reasons why more virtual processors aren't supported, so you might see poor performance. But there's nothing that would actually stop you.

—John Savill

InstantDoc ID 139926

Q: What's introspection as it relates to vShield and virtual machine (VM) anti-malware?

A: Traditional anti-malware technologies are sometimes poorly suited for virtual environments. Improperly tuned anti-malware processes can consume a lot of resources, such as processing power and memory, and can affect storage performance.

Offloading anti-malware activities away from the VM is a way to overcome these limitations. One mechanism to do this is introspection, a technique that uses a virtual platform's hypervisor layer to monitor VM activity from outside of the VM. The most noted product available that uses introspection is VMware vShield Endpoint, part of VMware's vShield security suite. Third-party solutions like Trend Micro's Deep Security can also integrate with vShield Endpoint. Projects in the public domain for the Xen Hypervisor are similarly available.

—Greg Shields

InstantDoc ID 139898

Q: I had to disconnect my Xbox 360 during an update, and now it won't start. What should I do?

A: The best solution is to download the latest firmware from Microsoft and burn it to a DVD or save it to a USB drive. Boot the Xbox from this media by having it present when you turn the Xbox on, and it should apply the update and resolve the problem.

—John Savill

InstantDoc ID 139913

Q: I'm using System Center Service Manager with a custom workflow that uses a trigger of a text value having new content added, but it's not working. Why not?

A: I recently had a custom workflow that I triggered based on the Notes attribute of a change request. Basically, my before criteria was that Notes didn't contain a text string, and the after criteria was that Notes contained a text string. However, the workflow never fired.

The problem was that the Notes value was initially empty, and the SQL query System Center Service Manager uses changes the "contain" workflow queries to a SQL LIKE command, which doesn't work against a null value. So the trigger fails.

The solution was to change the initial check (the before) to be if the Notes value was empty and the after check to be if Notes contained my text string. The workflow then triggered just fine. You might need to be careful about your logic, but the key point is that if your "before" value could be empty, don't try and use any of the contains logic.

—John Savill

InstantDoc ID 140022

Q: Will Fibre Channel storage eventually become obsolete in favor of Ethernet-based storage?

A: No one really knows if Fibre Channel storage will become obsolete, although there's a fairly good argument swirling around our industry that suggests it might. The argument has to do with how big the jumps in performance are for each technology. For Fibre Channel storage, each new generation gains speed that roughly corresponds with powers of two: 2GB to 4GB to 8GB, and then variants of 16GB.

On the other hand, Ethernet-based storage—which comprises iSCSI as well as Fibre Channel over Ethernet (FCoE)—has generally seen speed improvements across generations as powers of ten: 10MB becomes 100MB, which grows to 1GB, and then 10GB, 40GB, and eventually 100GB.

Graphing these maximum speeds over time shows Ethernet-based storage potentially far surpassing the maximum theoretical throughput for Fibre Channel.

—Greg Shields

InstantDoc ID 140357

Q: What's the role of VMware vCloud Connector?

A: Virtual Datacenter (vDC) resources that have been provisioned through VMware vCloud Director can be managed by end users via the vCloud Director agent. This agent exposes the appropriate actions an end user would require for administering their assigned resources.

Some organizations also manage vCenter resources on their own in addition to those provisioned by vCloud Director. For example, there might be some vCenter resources that you manage directly, while others you purchase from an external provider.

In these situations it can be easier to manage both types of resources beneath a single pane of glass. That unified management is possible using an add-on for vCenter Server called VMware vCloud Connector. The connector is a free download from VMware's website.

—Greg Shields

InstantDoc ID 139905

Q: What Office 2010 products can use Key Management Server?

A: Office 2010 is the first version of Office to support Key Management Server (KMS) use within an organization. A KMS key activates against the organization's internal KMS server infrastructure. The single Office 2010 KMS key activates the following products:

- Office 2010 Suite (any version)
- Office 2010 applications
- Microsoft Project 2010
- Microsoft Visio 2010

More details on KMS with Office 2010 can be found at Microsoft's TechNet site (technet.microsoft.com/en-us/library/ff678211.aspx).

—John Savill

InstantDoc ID 140675

Q: What is data center bridging (DCB) and what Ethernet extensions were created to support it?

A: Data center bridging (DCB) is describes the convergence of Fibre Channel storage atop traditional Ethernet-based devices. DCB specifically refers to four extensions to the Ethernet protocol that enable it to operate with the lossless nature of Fibre Channel traffic:

- Priority-based Flow Control (802.1Qbb), which enables the management of a single, bursty source on a multiprotocol link.
- Enhanced Transmission Selection (802.1Qaz), which enables bandwidth management between traffic types on multiprotocol links.
- Congestion Notification (802.1Qau), which addresses the problem of sustained network congestion by moving corrective actions to the network edge.
- Data Center Bridging Exchange Protocol (DCBX), which allows the automatic exchange of Ethernet parameters between switches and endpoints.

—Greg Shields

InstantDoc ID 140361

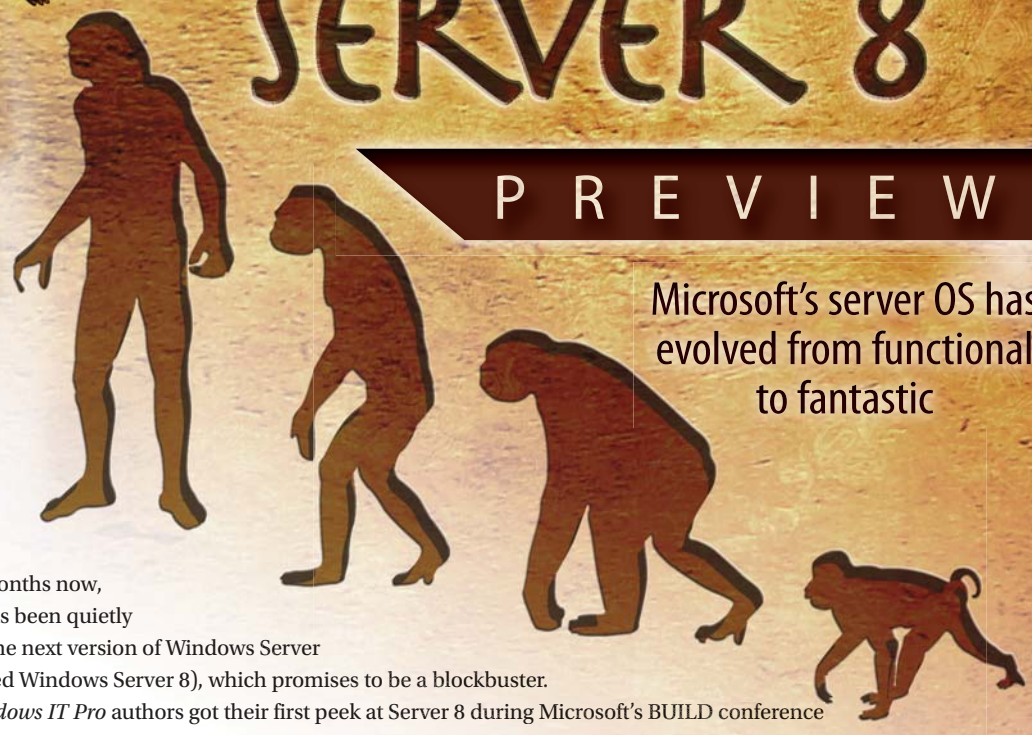
Q: If I have MBAM, can I store the BitLocker recovery key in Active Directory ?

A: Microsoft BitLocker Administration and Monitoring (MBAM) stores the recovery key in its SQL Server database. Although it's possible to store the recovery key in AD and in the MBAM SQL Server database store, the keys wouldn't stay synchronized once the recovery key was used. The key stored in AD would become invalidated, unless it was manually updated.

—John Savill

InstantDoc ID 140673

WINDOWS SERVER 8 PREVIEW



Microsoft's server OS has evolved from functional to fantastic

For several months now, Microsoft has been quietly revving up the next version of Windows Server (code-named Windows Server 8), which promises to be a blockbuster. Several *Windows IT Pro* authors got their first peek at Server 8 during Microsoft's BUILD conference in September. In this first look at the newest Windows Server OS, Paul Thurrott gives you the mile-high view, Sean Deuby covers Active Directory, Jeff James focuses on storage, and Michael Otey discusses virtualization.

Windows Server 8 is so big, so major a change, that it's difficult to conceptualize all at once. We can't even begin to cover all the changes here, and it will be weeks if not months before the weight of what's changing fully sinks in. But even at this early stage, it's clear that Microsoft is making monumental changes to Windows Server with this release—drawing a line in the sand that will divide the post–Server 8 world from the pre–Server 8 world. These changes are scary and exciting, but most of all, they're necessary. To get your own hands dirty with Server 8, go to www.buildwindows.com and download the Windows Developer Preview.

The Mile-High View — *Thurrott*

For the past decade or more, server management tools have largely focused on managing individual servers rather than the wider infrastructure of IT environments (i.e., groups of servers). One of Windows Server 8's main goals is to bring the centralized management of server infrastructure to the on-premises (and hybrid, or "cross-premises") world.

Server 8 is being built in tandem with Windows 8; they share the same code base and the same underlying platform advances and technologies. Although Microsoft hasn't publicized any release dates, I expect both OSs to ship by September 2012 at the latest. Microsoft has identified four key areas of advancement in Server 8: virtualization, centralized server management, modern workforce, and a new app platform—but I see things a bit differently.

As I already noted, the big-ticket item is the centralization of server management. In previous Windows Server releases, Microsoft provided two key technologies that virtually no customers actually use: Server Core and PowerShell.

Admins have been reluctant about Server Core for two reasons: Server Core supports only a limited set of roles and features (and can't be converted to the full Server version), and its command-line interface makes it difficult to use. We can run remotable admin tools against Server Core from other servers or from PC clients—but these tools aren't complete, and it's a bit ponderous to manually connect to different individual servers. Server 8 overcomes Server Core's limitations. Its new Server Manager is fully remotable and supports simultaneous management of multiple servers. The former Server Core (which might still be called Server Core in Server 8) is simply a mode that can be enabled and disabled on the fly.

Although PowerShell has its proponents, it still hasn't taken off with day-to-day admins and IT pros. In Server 8, PowerShell is integrated directly into Server Manager and other Server 8 admin tools, giving users an expandable pane that reveals the underlying PowerShell commands run behind the scenes during management tasks. This lets you copy and paste code to reuse later for your own automation scripts. PowerShell is also simplified, with better command auto-complete. Finally, the number of built-in PowerShell cmdlets jumps from around 200 in Windows Server 2008 R2 to more than 2,300 in Server 8. (For more information about PowerShell advancements, see Sean Deuby's "Administration Improvements" section in the "Active Directory Enhancements" section of this article.)

Server Manager has been recast as a tiles-based, Metro-style app that bears no relation to the previous version. It requires the full screen—as well as a high-resolution screen. The Microsoft Management Console (MMC) is still in Server 8 for legacy interfaces, but from what I understand, no new Microsoft admin GUIs will use the platform.

Where Server Manager falls apart is in the sub-screens that you visit when you need to actually get something done. The main Server Manager view is quite nice; it serves as a dashboard that provides you with a glanceable view of the overall health of your environment. But when you dive deeper, the UI is monochrome, indecipherable, and broken up into curious boxes of functionality. The content in these boxes is often interconnected, but it's not easily discoverable or usable. A painful example is the NIC Teaming interface: It requires you to select an object in one box (a server), then click a Tasks menu that's associated with another box (for network adapters), which is hidden until you mouse over it.

Microsoft's little lamented Windows Home Server product shipped with at least one major conceptual innovation: Via its Drive Extender technologies, users could ignore drive letters and pool local disk storage, accessing it as a single entity. Furthermore, Drive Extender offered a simple take on RAID's data redundancy functionality by duplicating all files on a second physical disk.

Drive Extender was a good idea, but the implementation wasn't exactly enterprise-ready. And after testing this technology on its new-generation small business servers, Microsoft discovered it wasn't compatible with many server apps and didn't work reliably. So it was scrapped, to the chagrin of Windows Home Server fans, many of whom have ignored the second-generation (and Drive Extender–less) Windows Home Server 2011 release.

But there was a reason behind this madness: Over in the core Server group, Microsoft engineers were working on storage innovations of their own. And although these changes might seem conceptually similar to Drive Extender, they're better and more reliably implemented in Server 8 (see Jeff James' "Storage" section of this article for more information).

—Paul Thurrott

InstantDoc ID 140666

Dynamic Access Control — *Deuby*

Closely related to storage, one of the big security challenges in a Windows domain environment is ensuring that files stored on NTFS volumes—all files, not just the ones you know about—have the correct security applied to them. According to Microsoft, despite the popularity of Microsoft Office SharePoint Server, file servers remain the largest repository of enterprise data (80 percent). Periodic audits for regulatory compliance are expensive and difficult to accomplish. Adding to this challenge is the fact that in the current Windows Server file environment, there's a gap between the overall information security policy and the actual boots-on-the-ground implementation of these policies on file servers throughout the domain. Anyone who has had to administer a server knows there are many opportunities for exceptions to slip through in an environment where tens, hundreds, or even thousands of file servers must be individually configured to meet corporate policy.

Windows Server 8 Dynamic Access Control is a new file-system authorization mechanism that gives IT the ability to define central file-access policies at the domain level that apply to every file server in the domain. Dynamic Access Control provides a "safety net," in addition to any existing share and NTFS permissions, which ensures that regardless of how the share and NTFS permissions might be changing on a day-to-day basis, this central overriding policy will still be enforced.

Dynamic Access Control marks the first incorporation of *claims* into the core Windows authorization (access control) model. A claim is an assertion about an object, issued by a trusted identity provider. Claims have existed for a while in the Internet security world, where they're at the core of federated identity technology. Claims are manipulated in this area by a Security Token Service (STS), such as Active Directory Federation Services (AD FS), which transforms data in Kerberos tokens into claims that can be consumed by web services.

In the Server 8 access control model, claims are Active Directory (AD) attributes that have been defined for use with central access policies. You can set claims for both users (User.company==FTE) and devices (Device.managed==true). This is easily done through the Active Directory Administrative Center (ADAC), where there's a new Claim Based Access container at the same hierarchy level as the domain. This kind of claim-based access gives you a degree of granularity and flexibility not available before. In fact, the product was originally named "claim-based access control" but was renamed to Dynamic Access Control because the new access control system has more to it than just claims.

Deploying centralized file-access policies through Dynamic Access Control is a four-part process. The first—and arguably the most difficult—step is to identify and classify file server data. These classifications are set by NTFS tags and require the file server to be running Server 8. This tagging can be done by several methods. Data can be tagged/classified based on application; by a sophisticated automatic mechanism that can, for example, search

The difference between networking and not working.

Some systems require you to reconfigure your network infrastructure to match their standards. Not the IBM BladeCenter® with Intel® Xeon® processors. It offers a broad range of networking technologies—including some of the most advanced virtualization solutions in the industry. So you can choose the one that works best with your infrastructure. And IBM BladeCenter can save you up to 40% on networking costs versus competitive offerings.[1]

intel Xeon inside™

Powerful. Intelligent.

Take 10 minutes to see for yourself.

Learn how you could achieve a 3-month ROI on your migration with our Systems Consolidation Tool. Visit ibm.com/systems/blade

1. The 40% cost savings are based on a comparison of the acquisition costs of 10 current generation HP rack optimized solutions (i.e., DL380 G7 Proliant with 10 GbE Ethernet and Fibre Channel infrastructure) to 10 current generation IBM BladeCenter and HS22 systems with converged fabric solutions from Brocade. See www-03.ibm.com/systems/bladecenter/hardware/openfabric/fcoe.html. The IBM solution includes chassis infrastructure. Pricing utilizes publicly available pricing per port for ToR ethernet and FC switching infrastructure as of Jan 2011. The 40% networking hardware costs savings result from eliminating separate Ethernet and Fibre Channel cards and switches in the deployment of an IBM BladeCenter FCoE solution for 10 servers and associated networking hardware in comparison to the HP solution. IBM, the IBM logo, ibm.com and BladeCenter are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml. Intel, the Intel logo, Xeon and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries.

for Social Security formats or the words "<your company> Confidential"; by folder; or it can be tagged manually by the file server content owner.

While this classification process is going on, Information Security can build central access policies that will apply to the different file classifications. These policies are far more flexible and specific than anything previously available in Windows access control; you can use expression-based access conditions with support for user claims, device claims, and file tags. When the policies are applied, there's a highly customizable Access Denied remediation mechanism that guides the user to a specific URL or generates an email message, to correct the situation if necessary.

After the policies are applied, you can also define centralized audit policies that can be applied across multiple files servers. Similarly to the access policies, these audit policies are defined with expression-based auditing conditions with support for user claims, device claims, and file tags. And because there's a big gap between a policy as it's initially thought up and how it looks when it hits the real world, there's a built-in mechanism that works like Group Policy's Resultant Set of Policy (RSoP) to test against the target file servers in what-if simulations before the policies are ever activated.

Finally, you can choose to automatically protect certain types of Microsoft Office data classifications with Windows Rights Management Services (RMS) based on file tagging. Part of Dynamic Access Control, this capability doesn't require a separate Active Directory Rights Management Services (AD RMS) installation. RMS provides near real-time protection within a few seconds of when the document is tagged. Dynamic Access Control also has extensibility to protect non-Office RMS protectors.

A lot of work had to be done to various Windows components to make this high-level capability work. AD had to be updated to comprehend claims. NTFS was updated to be able to use *regular expressions* (en.wikipedia.org/wiki/Regular_expression) in file system ACLs, in addition to security principals such as users and groups. This is a huge added value for administrators, because after they upgrade to Server 8, they can immediately take advantage of the extra flexibility this provides—even if no centralized policies have been configured. For example, using regular expressions, you can easily create the equivalent of ANDing groups together; in previous versions, you could only OR them together. For instance, you can express directly that to access a certain set of files you must be a member of the Full-Time Employees group AND a member of the Finance group, without having to create all the nested groups (Finance group is nested in Full-Time Employees group is nested in Domain Users) required in the current model.

Modifications to the core authentication platform are critical to making Dynamic Access Control work. To make claims available to the new access control model without redesigning AD authentication, claims are stored in the Privilege Attribute Certificate (PAC) field inside the Kerberos ticket. This is the same place where the user's SID and group membership SIDs are stored, so it would seem that extracting claim information would be a fairly straightforward process. The downside of this design choice is that the PAC has a limited size, and some companies are running up against token-bloat issues when a user is a member of too many groups. Of course, the additional flexibility of Dynamic Access Control will hopefully reduce the number of groups a user must be a member of.

Dynamic Access Control in Server 8 is limited to the NTFS file system. Why? As it was described to me by Robert Deluca, Microsoft senior program manager, Server 8 was designed by scenario-based engineering, and the most compelling initial scenario to solve was that of centralized access control and compliance. Microsoft is starting with this scenario, and as the company gains experience with this release, it might expand to encompass other areas (such as claims-based authentication and authorization).

Server 8's Dynamic Access Control isn't just a powerful security and compliance feature. It's also a basis for more authorization flexibility in future versions of Windows. And probably to the relief of IT pros concerned about job security, implementing it will be a good-sized project to keep them busy for quite a while.

—Sean Deuby

InstantDoc ID 140572

Active Directory Enhancements — *Deuby*

Active Directory (AD) is a foundational part of the Windows Server system, and any changes to it must address three broad sets of requirements. The first requirement set is for the entire Windows Server ecosystem that depends upon it for authentication and access control. Whether it's Microsoft Exchange Server, System Center, Hyper-V, SQL Server, or many other products inside and outside of Microsoft, thousands of enterprise software solutions depend on AD.

The second set of requirements is for AD service owners—the systems administrators who actually manage the AD distributed application across its span of domain controllers (DCs). Although AD has made great strides in manageability since its early days, it still remains a complicated beast (perhaps a hydra with its many heads). How can this critical but confusing piece of infrastructure be made easier to work with in an IT environment that's far more complicated than when the directory service was first designed?

The third set of requirements is for the literally millions of users around the world who work with AD directly or indirectly for access control to various resources in their domain. How will the aging users/groups model of access control evolve to meet the complex security and compliance requirements we live with today, as well as grow for tomorrow's certainly expanding needs? As Microsoft's Nathan Muggli said, "Designing changes to Active Directory is like ordering pizza for a million people; everyone wants something different."

For Windows Server 8, the AD team didn't alter the product dramatically. There's no SQL Server–based directory service database, nor can a DC host more

than one domain partition. (Why would you need to anymore, when you can create another virtual DC?) Instead, the team focused on three major goals that address all of its stakeholders to varying degrees. First, AD needs to have virtualization that just works. Second, AD must be simple to deploy. Finally, AD must also be simple to manage.

Virtualization that Works

Ensuring that AD virtualization works should be a great relief to many systems administrators, because even though the rules for a safely virtualized AD aren't that difficult, the responsibility is spread across several teams. This means that keeping AD safe in a virtual world isn't just a technical problem; it's a people or organizational problem. And the consequences for screwing it up can be severe, as illustrated in the Microsoft article "USN and USN Rollback" at technet.microsoft.com/en-us/library/virtual_active_directory_domain_controller_virtualization_hyperv(WS.10).aspx.

What causes problems for AD before Server 8 in a virtualized environment is that the AD distributed application isn't aware of any virtualization-specific actions taken underneath it at the host level. Specifically, you can confuse AD and potentially induce an unhealthy condition known as USN rollback if you restore a DC virtual machine (VM) from a snapshot or image backup. Why? Because a distributed application such as AD has more off-server dependencies than a single-instance application. When a DC has been restored from an image backup, it magically appears as though it's from an earlier time—but in an incomplete manner because neither its partners nor the restored DC itself recognizes it.

In contrast, Server 8's "virtualization-safe" AD technology ensures that a virtual DC is able to detect when snapshots are applied or a VDC has been copied. Detection of these changes is built on what's known as a VM generation ID (gen ID) to detect changes and protect AD, or take corrective measures. This requires changes to Hyper-V, and Microsoft is working with other virtualization vendors to make sure they include this technology in the latest version of their hypervisors as well. It's in their best interest to do so, because until then Microsoft has a competitive advantage in its own Hyper-V.

Domain Controller Cloning

The team's second goal of making AD simple to deploy was made possible by the gen ID technology, which makes it easy to safely clone virtual Server 8 DCs. From an administrator's viewpoint, the process is pretty simple: You copy/paste/rename the source virtual DC's .vhd disk file to create a second copy on disk, relocate it to the destination folder you desire, use Hyper-V Manager or Virtual Machine Manager to create a new VM, and associate the copied VHD with the new VM. Then, you just start it up. (There's more that happens under the covers, of course.)

Upgrades and DCPROMO Made Simple

In addition to being able to clone VDCs, the upgrade and promotion process has been completely reworked and made far simpler. In Server 8 AD, you can upgrade your domains and forest from a previous AD version to the Server 8 version entirely from Server Manager. Unlike with previous versions, you don't have to log on to different DCs with different sets of credentials, find the correct version of ADPREP, run /FORESTPREP in the forest, run /DOMAINPREP in each domain, and choose when to update SYSVOL—it's all taken care of for you. (If you want to run an *a la carte* upgrade step by step, that's still available.) The DCPROMO process has also been simplified and includes significant built-in troubleshooting, because this area was one of the highest call generators to Microsoft Customer Service and Support (CSS).

Administration Improvements

The third goal of Server 8 AD is to make it easier to manage. In keeping with the pervasive PowerShell management theme found throughout the OS, it's now possible to do pretty much any administrative task in AD with PowerShell. Because PowerShell has increased its coverage of administrative tasks from 200 to more than 2,300 cmdlets, this actually makes your life easier because instead of having to script up a number of PowerShell cmdlets to get something done, you can probably find a dedicated cmdlet for what you want to do.

Although other AD actions have been PowerShell-ized, interestingly, the AD Recycle Bin (which is a welcome addition to Windows Server 2008 R2 that was PowerShell only) has gained a GUI. Personally, I'm all for a Recycle Bin GUI; when someone has fat-fingered an account or group into oblivion, no one wants to spend time looking for the PowerShell syntax to restore it!

In addition, the Server 8 Active Directory Administrative Center (ADAC) has a new pane at the bottom called the PowerShell History Viewer. Although it's hidden by default, you can expand the History Viewer pane to see which PowerShell commands run under the covers as a result of the actions you're taking in ADAC. This way, you can learn the syntax of AD-related PowerShell cmdlets by watching them flow by. You can also easily copy the cmdlets to paste them into a script of your own or combine cmdlets into tasks with the Tasks feature in the pane. The history is retained between ADAC sessions, so you can go back days to find the syntax of a particular command you ran previously. By the way, the venerable Active Directory Users and Computers (ADUC) console isn't going away anytime soon, because it has extensibility that ADAC currently lacks—but ADUC isn't being enhanced. An appropriate maxim might be, "ADUC is dead; long live ADAC!"

Active Directory–Integrated Product Activation

Another feature that falls under the "easy to manage" goal is something that simply makes sense: Product activation now uses AD instead of a separate infrastructure. It uses LDAP for communication with its clients instead of RPC, and no data is written back to the directory. You won't be getting rid of Key Management Service (KMS) for a while, though; it's still required for down-level licensing (i.e., everything that's in production today).

AD FS Takes One More Step Toward Active Directory Integration

Active Directory Federation Services (AD FS) has become a little more integrated into the mainstream server bits than its previous releases. In Server 8, AD FS is installed as a role within Server Manager instead of

as a downloadable add-on. It hasn't yet taken the much-larger architectural step of becoming an AD component, but it's a step in the right direction. With the addition of claims into the Kerberos token, AD FS will be able to extract and use these claims from the token, as well as use static device claims (e.g., which department a notebook belongs to).

Making Active Directory Easier

Server 8 AD has several much-appreciated improvements in virtualization, deployment, and management designed to ease the frustration and support headaches of the tens of thousands of IT pros who aren't dedicated AD specialists. These improvements help "lower the friction of deployment" of Windows Server (to quote Jeffrey Snover). And many smaller changes to AD are underpinnings for a wide variety of new features in the OS. As the product goes into full beta, it'll be interesting to see what tweaks and adjustments are made to one of Microsoft's most widely deployed enterprise applications.

—Sean Deuby

InstantDoc ID 140571

Storage — *James*

Windows Server 8 has a ton of all-new storage features, as well as many improvements to existing features. I focus on the following three: storage pools and spaces, improvements to CHKDSK, and data deduplication.

Storage Pools and Spaces

With many IT environments filled with a huge array of storage devices of varying types and sizes, finding a way to easily manage and allocate that storage has historically been an onerous task. Microsoft hopes to change that with storage pools and storage spaces, two new Server 8 storage abstraction concepts.

You can think of storage pools as units of storage aggregation that provide administration and isolation. Storage spaces give virtual disks performance, resiliency, and simplified storage provisioning.

As an example, you can use storage spaces to aggregate individual storage devices into a single unit of storage, then provision and divvy up that storage space as you see fit. It's a powerful way to provide storage for virtual machines (VMs) that greatly simplifies management of disparate storage types. Storage pools and spaces can also scale all the way from small-to-midsized businesses (SMBs) up to the largest enterprises, which promises a new level of storage flexibility.

CHKDSK Redux

The venerable CHKDSK has been around in some form or another since the days of MS-DOS and has been the bane of many systems administrators' existence. Running on larger storage volumes, a CHKDSK process can sometimes take hours to complete, which can throw the best-laid plans of even the most organized IT professional into the toilet. Microsoft seems to have finally heard the psychic anguish of millions of IT pros crying out when the dreaded CHKDSK message appeared; some long-overdue improvements are in store for CHKDSK in Server 8.

The biggest news is that CHKDSK scanning is split into two separate phases: an "online" scan and corruption-logging phase in which CHKDSK searches volumes for defects behind the scenes, and a vastly shortened "offline" fixing phase that only corrects defects in drive data.

At the Windows Server 8 Reviewers Workshop, Matt Garson, Microsoft senior program manager for storage and file systems, gave a compelling demonstration of how much time the new CHKDSK can save over the old version: Scanning 300 million files with the old CHKDSK could take 350 minutes, whereas the same number of files in the new version takes less than 8 seconds. This improvement in speed is amazing, and it shows that Microsoft isn't just focusing on producing shiny new features in Server 8 but is also addressing some Windows Server features that have frustrated systems administrators for years.

Data Deduplication

With demand for physical storage increasing exponentially, one way to reduce storage demands is to rely on technologies such as data deduplication, which Microsoft leverages in Server 8 to reduce file storage sizes. Here's how it works: Suppose you have dozens of virtual hard disk (VHD) files. Many of the files on those VHDs are identical copies of each other, such as Microsoft Paint. Data deduplication removes all the copies of Microsoft Paint from all those VHDs but one, puts all that redundant data into a separate store in System Volume Information (SVI), then simply leaves a marker that points to the file that serves as the template. Imagine this used across thousands (if not millions) of files and throughout your storage network, and you can expect to see vast reductions in storage space.

I went through a hands-on Windows 8 lab at the Reviewers Workshop to test data deduplication, and I was impressed to discover that the technology also works across networks to separate Server 8 or Windows 8 machines. The time it takes to copy files is vastly reduced. This impressive feature should do wonders for storage efficiency and network utilization. Perhaps this is the first of the many "better together" features of Server 8 and Windows 8.

—Jeff James

InstantDoc ID 140577

Virtualization — *Otey*

Clearly, there have been huge enhancements to Windows Server 8 in multiserver management, PowerShell automation, Active Directory (AD), and storage. However, the biggest changes might actually be in Server 8's new Hyper-V 3.0 virtualization support. At Microsoft's recent Windows Server 8 Reviewers Workshop, Jeff Woolsey, principle program manager lead for Windows virtualization in Microsoft's Windows Server and Cloud division, presented the new features in

the next version of Microsoft's Hyper-V virtualization platform. In the introduction to the Reviewers Workshop, Jeffrey Snover, distinguished engineer and lead architect for the Windows Server division, made the bold statement that Microsoft really gets it right in the third release. This is definitely true of the upcoming version of Hyper-V: Server 8's Hyper-V 3.0 finally closes the technology gap with VMware's vSphere.

Hyper-V 3.0 Scalability

The days when Hyper-V lagged behind VMware in terms of scalability are a thing of the past. The new Hyper-V 3.0 meets or exceeds all of the scalability marks that were previously VMware-only territory. Hyper-V 3.0 hosts support up to 160 logical processors (where a logical processor is either a core or a hyperthread) and up to 2TB of RAM. On the virtual machine (VM) guest side, Hyper-V 3.0 guests will support up to 32 virtual CPUs with up to 512GB of RAM per VM. More subtle changes include support for guest Non-Uniform Memory Access (NUMA), where the guest VM has processor and memory affinity with the Hyper-V host resources. NUMA support is important for ensuring scalability increases as the number of available host processors increases.

Multiple Concurrent Live Migration and Storage Live Migration

Perhaps more important than the sheer scalability enhancements are the changes in Live Migration and the introduction of Storage Live Migration. Live Migration was introduced in Hyper-V 2.0, which came out with Windows Server 2008 R2. Although it filled an important hole in the Hyper-V feature set, it wasn't up to par with the VMotion capability provided in vSphere. Live Migration was limited to a single Live Migration at a time, whereas ESX Server was capable of performing multiple simultaneous VMotions. In addition, vSphere supported a similar feature, called Storage VMotion, which allowed a VM's storage to be moved to new locations without incurring any downtime. Hyper-V 3.0 erases both of these advantages. Hyper-V 3.0 supports multiple concurrent Live Migrations. There are no limits to the number of concurrent Live Migrations that can take place with Hyper-V 3.0. In addition, Hyper-V 3.0 also provides full support for Storage Live Migration where a VM's files (i.e., the configuration, virtual disk, and snapshot files) can be moved to different storage locations without any interruption of end-user connectivity to the guest VM.

Microsoft also threw in one additional twist that vSphere has never had. Hyper-V 3.0 has the ability to perform Live Migration and Storage Live Migration without the requirement of shared storage on the back end. The removal of this requirement really helps bring the availability advantages of Live Migration to small-to-midsized businesses (SMBs) that can't afford a SAN or don't want to deal with the complexities of a SAN. The ability to perform Live Migration without requiring shared storage really sets Hyper-V apart from vSphere and will definitely be a big draw—especially for SMBs that haven't implemented virtualization yet.

VHDX, ODX, Virtual Fibre Channel, and Boot from SAN

Another important enhancement with Hyper-V 3.0 is the introduction of a new virtual disk format called VHDX. The new VHDX format breaks the 2TB limit that was present in the older VHD format and pushes the maximum size of the virtual disk up to 16TB per VHDX. The new format also provides improved performance, support for larger block sizes, and better resilience to corruption.

Hyper-V 3.0 also supports a feature called Offloaded Date Transfer (ODX). This feature lets Hyper-V take advantage of the storage features of a back-end shared storage subsystem. When performing file copies on an ODX-enabled SAN, the OS hands off all the data transfer tasks to the SAN, providing much higher file copy performance with zero to minimal CPU utilization. There's no special ODX button. Instead, ODX works on the back end. ODX does require the storage subsystem to support the new ODX specifications.

Companies that use Fibre Channel SANs will appreciate the addition of virtual Fibre Channel support in Hyper-V guests. Hyper-V 3.0 guests can have up to four virtual Fibre Channel host bus adapters (HBAs). The virtual HBAs appear in the VMs as devices, much like virtual NICs and other virtual devices. Hyper-V 3.0 VMs will also have the ability to boot from an iSCSI SAN.

Extensible Virtual Switch and NIC Teaming

In keeping par with the sweeping changes in Hyper-V's compute capabilities and storage, Microsoft also made significant enhancements to Hyper-V's networking capabilities. First, the company updated the virtual switch that's built in to the Hyper-V hypervisor. The new virtual switch has a number of new capabilities, including multi-tenant support, as well as the ability to provide minimum and maximum bandwidth guarantees. In addition to these features, the new virtual switch is also extensible. Microsoft provides an API that allows capture, filter, and forwarding extensions. To ensure the high quality of these virtual switch extensions, Microsoft will be initiating a Hyper-V virtual switch logo program.

Another overdue feature that will be a part of Server 8 is the built-in ability to provide NIC teaming natively in the OS. VMware's ESX Server has provided NIC teaming for some time. Prior to Server 8, you could get NIC teaming for Windows only via specialized NICs from Broadcom and Intel. The new NIC teaming works across heterogenous vendor NICs and can provide support for load balancing as well as failover.

The Magic Number 3

As Jeffrey Snover pointed out, 3 does seem to be Microsoft's magic number—at least for Hyper-V. Hyper-V 3.0 brings Microsoft's virtualization on par with VMware's vSphere. Businesses that are just getting into virtualization or that are balking at VMware's latest price increases will find Hyper-V to be a very cost-effective and highly competitive alternative.

—Michael Otey

InstantDoc ID 140573

Paul Thurrott (paul@windowsitpro.com) | Sean Deuby (sean@windowsitpro.com)
Jeff James (jjames@windowsitpro.com) | Michael Otey (motey@windowsitpro.com)

Active Directory Rights Management Services

Use AD RMS for secure collaboration

by Jan De Clercq

Cloud computing increases data mobility and exposure. Corporate data is at risk when it travels the private and public parts of a cloud and data owners ignore the exact cloud location where corporate data is stored or processed. To properly deal with these challenges, organizations need flexible data security tools that let them enforce granular access control to ensure that only authorized users, business partners, cloud service providers, and customers can access their information.

In this context, it's worthwhile to consider enterprise rights management (ERM) solutions such as Microsoft Windows Rights Management Services (RMS). To prevent unauthorized access, RMS encrypts information and enforces a granular access-control mechanism that decides whether and how it releases information to a user. The protection RMS provides is persistent and travels with the information no matter where it goes on your network or in the cloud.

Microsoft bundles RMS with Windows Server 2008, Windows 7, and Windows Vista. This is RMS version 2—officially called Active Directory Rights Management Services (AD RMS). Microsoft provided RMS version 1 as a free add-on to Windows Server 2003, Windows XP, and Windows 2000 Workstation. RMS protection can be added to Microsoft Office 2010, 2007, and 2003 documents; Microsoft Outlook email messages; and Microsoft PowerPoint, Excel, Word, and InfoPath documents. RMS can also secure XPS-formatted files. RMS support for other document formats (e.g., Adobe Acrobat PDF, Microsoft Office 2000, Microsoft Visio) can be added through special plug-ins that are available from third-party software vendors such as GigaTrust.

You can use RMS to secure information exchanges between different organizations and cloud entities. To do so, you can consider several architectural options.

Overview

RMS provides the following four options for the exchange of RMS-protected documents between organizations:

- Use a single RMS infrastructure and create external accounts for your partner in your AD infrastructure.
- Create an RMS infrastructure at the partner's site and set up an RMS trust between yours and your partner's RMS infrastructures.
- Leverage Windows Live ID credentials for authenticating external users.
- Use identity federation by leveraging Active Directory Federation Services (ADFS) or the Microsoft Federation Gateway.

To configure RMS for external collaboration, you must use the Trust Policies container in the Microsoft Management Console (MMC) Active Directory Rights Management Services snap-in,

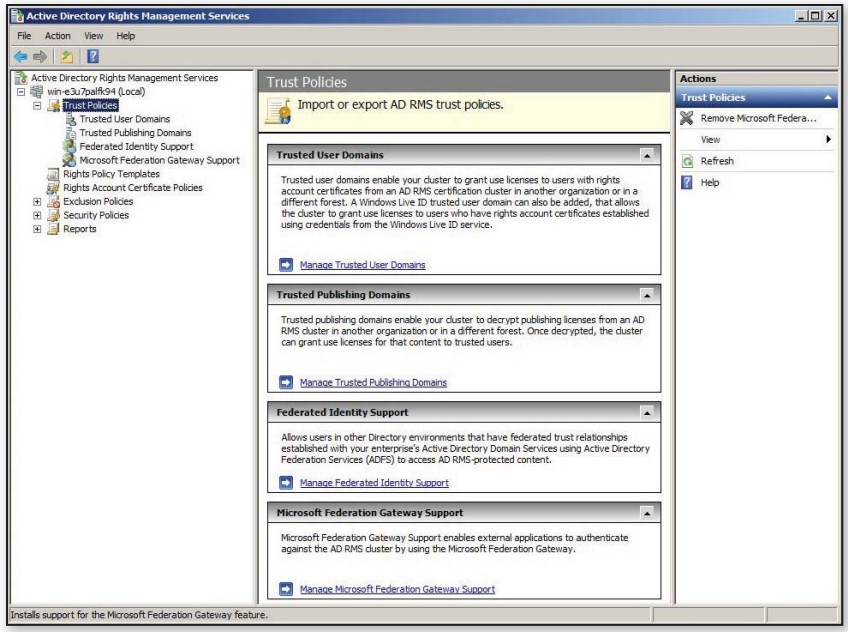


Figure 1: Configuring RMS for external collaboration

which Figure 1 shows. By default, this container has two subcontainers: Trusted User Domains and Trusted Publishing Domains. If you select the Identity Federation Support role service during installation of the RMS server, the Trust Policies will have a third subcontainer called Federated Identity Support. Finally, if your RMS server runs on Windows Server 2008 R2 SP1, a fourth container called Microsoft Federation Gateway Support will show up in the Trust Policies container. You can also use Windows PowerShell commands to configure all RMS trust policy settings, as described in the Microsoft TechNet article "Establishing Trust Policies" at technet.microsoft.com/en-us/library/ee221019(WS.10).aspx.

Single RMS Infrastructure

Using a single RMS infrastructure saves your partner the effort and cost of setting up an RMS infrastructure but requires you to create external accounts for your partner in your AD infrastructure, thus adding provisioning and de-provisioning complexity and account management overhead. Because each user will get another account and associated credentials to remember and maintain, this approach also isn't the most user-friendly integration option.

To enable partner users to access and create RMS-protected content, your organization must also publish RMS externally, to either the Internet or an extranet. The Microsoft TechNet article "Internet Access Considerations," which is a chapter in the RMS documentation at technet.microsoft.com/en-us/library/dd996655(WS.10).aspx, provides good guidance for publishing RMS externally.

Your partner organizations must also make sure their users install the AD RMS client software and use RMS-enabled Office applications. If your partners only want to access protected content (and not create new protected content), they can also use the Rights Management Add-On for Internet Explorer (RMA), available at www.microsoft.com/download/en/details.aspx?id=4753. In this case, your partner doesn't need to install the RMS client and RMS-enabled applications on its client computers. When you plan to deploy RMA in your organization, I advise you to read the Microsoft article "Introducing Rights-Managed HTML" at download.microsoft.com/download/c/b/0/cb07013e-7630-47c3-9237-cc839ee5fd61/RMH%20Intro.doc.

> Using a single RMS infrastructure adds provisioning complexity and account management overhead.

RMS Trust Relationships

An RMS trust relationship is an RMS-specific trust that's different from an AD trust and that's created between two RMS installations. A key condition for an RMS trust is that your partner has deployed an RMS infrastructure—which is a rather heavy infrastructure requirement that you can't impose on every partner.

You can define an RMS trust from the Active Directory Rights Management Services snap-in. In the Trust Policies container, you'll see two options for setting up an RMS trust: You can either use a trusted user domain (TUD) or a trusted publishing domain (TPD).

- When you use a TUD, your RMS cluster can issue RMS use licenses to users that were authenticated by another RMS cluster. You can add a trusted user domain by importing the Server Licensor Certificate (SLC) of the RMS cluster in the other organization on your RMS cluster.
- When using a TPD, you let your AD RMS server issue RMS use licenses to users that have a publishing license that was issued by another RMS server. You can add a trusted publishing domain by importing the SLC and the associated private key of the RMS server in the other organization on your RMS server.

Both TUD-based and TPD-based RMS trust relationships are unidirectional. The creation of an RMS trust requires no direct connection between the AD RMS clusters or the AD forests—it can be done out-of-band by exchanging the required certificates and/or keys.

However, when you use a TUD, for the external user to obtain an RMS use license from your RMS cluster, your RMS server must be accessible from the Internet or from the extranet. Again, "Internet Access Considerations," at technet.microsoft.com/en-us/library/dd996655(WS.10).aspx, provides good setup guidance. This external access isn't a requirement for a TPD-based RMS trust relationship. In that case, external users can get an RMS use license for your protected RMS content from their organization's RMS servers.

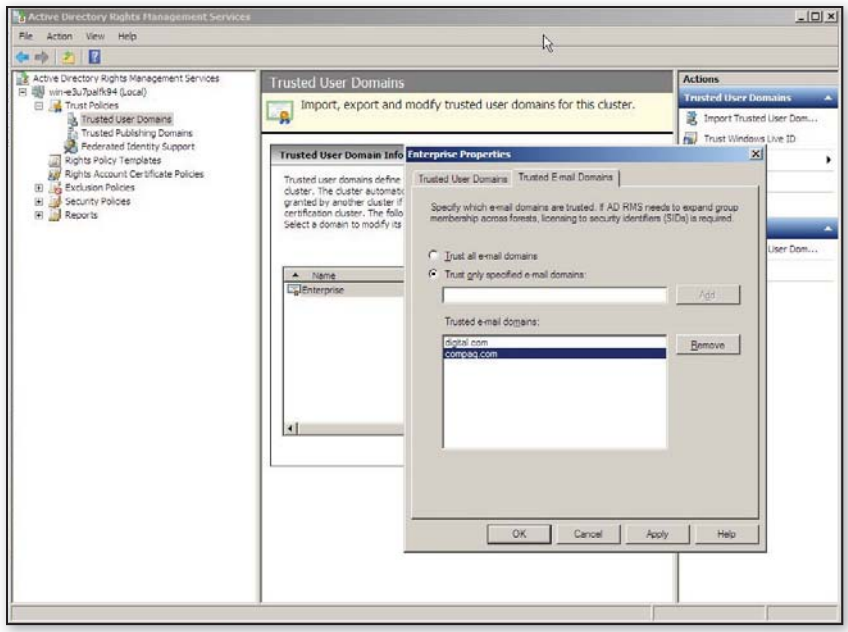


Figure 2: Configuring trusted email domains

For a TUD-based RMS trust relationship, you can optionally exclude certain email subdomains and their users from obtaining RMS use licenses from your RMS cluster. You can do so from the properties of the TUD certificate that shows up in the middle pane of the Active Directory Rights Management Services snap-in, as Figure 2 shows.

Windows Live ID

Windows Live ID is an Internet-based authentication infrastructure that's run by Microsoft. To leverage Windows Live ID credentials for authenticating external users to your RMS servers, the partner accounts that want to read RMS-protected content must have a registered Windows Live ID account. Some organizations are reluctant to use Windows Live ID credentials for authentication when the credentials are used for accessing internal (possibly very confidential) data. Windows Live ID performs only a very basic identity assurance check (based on the use of a valid email address) when a user requests a Windows Live ID account.

To enable Windows Live ID authentication in RMS, you must set up a trust with Microsoft's online RMS service—which is basically a service that can provide an RMS authentication certificate (or rights account certificate—RAC—in RMS terms) to Windows Live ID–authenticated users. Setting up this trust will enable Windows Live ID recipients to read your protected content but not create RMS-protected content.

To enable users with a Windows Live ID RAC to obtain RMS use licenses from your internal RMS cluster, you must set up a TUD for Windows Live ID in your RMS configuration. You can do this from the \Trust Policies\Trusted User Domains container in the Active Directory Rights Management Services snap-in. In the Actions pane, select Trust Windows Live ID. If the trust creation is successful, the Windows Live ID certificate will appear in the Trusted User Domain list in the middle pane, as Figure 3 shows.

As for any other RMS TUD, you can exclude certain Windows Live ID domains and their users from obtaining RMS use licenses from your RMS cluster. You do so from the properties of the Windows Live ID certificate that appears in the middle pane.

To make Windows Live ID authentication to RMS work, you must also make a configuration change on your RMS IIS web server to give external Windows Live ID users access to the AD RMS licensing web service. You do so by allowing anonymous access on the licensing web service. By default, the licensing service is configured to use Windows Integrated Authentication.

Identity Federation

Microsoft provides two identity federation–based technologies to enable the exchange of RMS-protected content between organizations: The first is based on ADFS, whereas the second leverages the Microsoft Federation Gateway. At press time, the second solution could only be used to exchange RMS-protected mail content between Microsoft Exchange Server and Outlook users in different organizations.

ADFS is the identity federation solution that Microsoft introduced in Windows Server 2003 R2. ADFS provides services to create trust relationships between

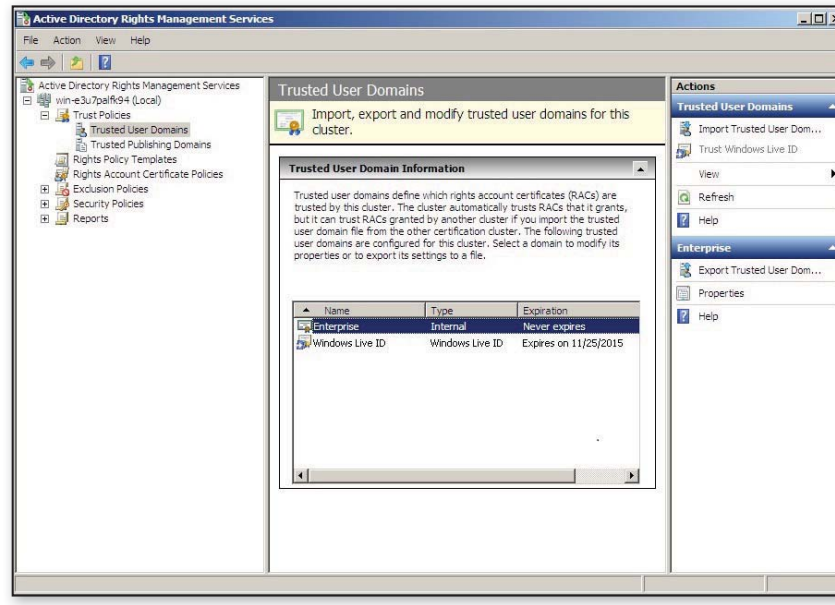


Figure 3: Setting up a TUD for Windows Live ID in RMS

organizations and to allow for easy resource access between them. For example, you can use ADFS to provide a web single sign-on (SSO) experience to external partners that access documents on your web portal. Thanks to ADFS, partners can authenticate to their AD infrastructure using their internal accounts and then transparently access the documents on your portal. ADFS can translate the partners' authentication tokens into a format that can be understood by your organization's ADFS servers, which can then give the partners transparent access to the resources on your portal.

RMS can also leverage ADFS to give external users access to internal RMS-protected data. ADFS integration is possible only with RMS version 2 (the version that Microsoft ships with Server 2008 and later); only this version is an ADFS claims-aware application. On the ADFS side, the RMS integration can work with both ADFS version 1 and version 2.

The ADFS support in RMS allows organizations to securely share their RMS-protected content with other organizations even if these organizations don't have an internal RMS infrastructure. However, this scenario requires a complete ADFS infrastructure, as follows:

- To use ADFS with RMS, your organization must have an internal ADFS infrastructure, as well as have an ADFS trust in place with each of the partners with which you want to exchange RMS-protected data. Also, you must install and enable Federated Identity Support on your RMS servers, as the Microsoft TechNet article "Configure Federated Identity Support Settings," at technet.microsoft.com/en-us/library/cc732627(WS.10).aspx, explains.
- Your partners must run Windows 2003 R2 or later, have their own ADFS infrastructure, and install the RMS client on their client platforms.

It's also worth pointing out that some Microsoft applications can't use ADFS (yet) and thus can't be used for creating or accessing RMS-protected content based on ADFS authentication. These applications include Microsoft Office SharePoint Server, Windows Mobile, and the XPS viewer. SharePoint and Windows Mobile have the same problem with Windows Live ID authentication.

In addition, ADFS and Windows Live ID can't use groups—only individual user accounts—to protect or access RMS content. This relates to the ability of performing group expansion when these authentication methods are used. Microsoft made some changes to ADFS in Server 2008 R2 that do enable RMS group expansion from this platform on. For more information about these two problems, see the Microsoft TechNet article "Assessing the Alternatives for Sharing Protected Documents Between Organizations" at technet.microsoft.com/en-us/library/dd983942(WS.10).aspx.

Microsoft provides detailed guidance on how to set up RMS-ADFS integration. See the TechNet article "AD RMS with AD FS Identity Federation Step-by-Step Guide" at technet.microsoft.com/en-us/library/cc771425(WS.10).aspx.

The second identity federation–based solution—the Microsoft Federation Gateway—is an identity broker that Microsoft makes available in the cloud. The advantage of a gateway solution is that organizations must manage only a single identity federation trust relationship (with the Microsoft Federation Gateway) to enable their identities to access all other services that are federated with the gateway. The scope of the federation can be further controlled from the RMS management interface by creating allow or deny lists of users and domains for licensing and by specifying the domains that can receive publishing licenses.

Microsoft Federation Gateway support for RMS requires Server 2008 R2 SP1 on your RMS servers. Remember that (at press time) the only application that can take advantage of the Microsoft Federation Gateway for the exchange of RMS-protected data between organizations is Exchange Server 2010. You can find more information about installing and configuring Microsoft Federation Gateway support in the Microsoft TechNet article "AD RMS Microsoft Federation Gateway Support Installation and Configuration Guide" at technet.microsoft.com/en-us/library/gg636976(WS.10).aspx.

Diff'rent Strokes for Diff'rent Folks

Microsoft RMS provides different options to securely exchange documents between organizations. An important consideration for selecting the correct RMS collaboration setup is the availability of an RMS and ADFS infrastructure in your organization and your partners' organizations.

The advantage of a gateway solution is that organizations must manage only a single identity federation trust relationship to enable their identities to access all other services that are federated with the gateway.

The collaboration approach that offers the most complete feature set is an RMS trust (TUD or TPD). Federation is a good approach if you can live with the restricted application support. For a limited number of external users, Windows Live ID is the simplest option. If the number of external users is larger, creating user accounts in your local Active Directory (AD) can be the best option. However, in such a scenario you must take into account the overhead of provisioning and managing these accounts.

InstantDoc ID 140326

Jan De Clercq
(jan.declercq@hp.com) is a member of HP's International Expertise Team and focuses on architecture for Microsoft-based IT infrastructures, identity management, cloud computing, and security. He's co-author of *Microsoft Windows Security Fundamentals* (Digital Press).

What's New: Exchange Server 2010 & Remote PowerShell

EMS improves Exchange's scriptability

by Paul Robichaux

It might seem a little odd to write a "what's new" article about any aspect of Microsoft Exchange Server 2010, given that it has been out for almost 2 years now. It's true that many aspects of Exchange 2010 have been covered in great detail. However, the changes to the Exchange Management Shell (EMS) haven't been covered in great detail. These changes are significant because EMS underlies and is intertwined with Exchange management at every level. All the GUIs you see in Exchange are built on top of EMS, and everything you can do in the Exchange Management Console (EMC), from the command line, or from the Exchange Control Panel (ECP) ultimately relies on the correct execution of EMS. For the purposes of this article, I assume you're somewhat familiar with EMS in either Exchange 2010 or Exchange 2007. The article focuses on new features and changes in Exchange 2010, so if you're a complete PowerShell beginner, you might find the online Learning Path (windowsitpro.com, InstantDoc ID 140284) to be helpful.

PowerShell Architecture

You can't really tell from just looking at its character-based interface, but PowerShell is actually a very sophisticated piece of engineering. Its designers wanted to replace the traditional Windows Command-Line Interface (CLI) with something better: something that combines the expressive power of previous CLI implementations such as DEC VMS, the rich composition ability of UNIX shells, and the ability to manipulate objects that represent things in the system, as opposed to mere text on screen.

To do this, the PowerShell team built a language interpreter, a runtime, and a set of interfaces that allow PowerShell cmdlets to call native Windows services. On top of this, the Exchange team built a large set of Exchange-specific cmdlets that let us directly interact with and manage various parts of Exchange. Web Figure 1 (windowsitpro.com, InstantDoc ID 140284) shows EMS's layered architecture.

In Exchange Server 2007, EMS commands are executed locally. In Exchange 2010, EMS commands are executed across the network. This is possible because of a new component known as Windows Remote Management. WinRM is Microsoft's implementation of an Internet-standard management protocol known as Web Services for Management (WS-MAN). (For information about other related standards, see the Distributed Management Task Force—DMTF—website at www.dmtf.org/standards.) Microsoft included WinRM support in Windows Vista, Windows Server 2008, and later OSs, as well as making a downloadable runtime available for other Windows versions. If you're familiar with Windows Management Instrumentation (WMI), then the concept behind WinRM will be very familiar: It's designed to provide a network-based management layer that Microsoft's own management tools can use to query and change various system parameters across the network. The difference is that because WinRM is based on WS-MAN instead of Microsoft's own proprietary standard, it offers a higher degree of interoperability. PowerShell uses WinRM to send commands remotely to other Exchange servers on the network. The actual implementation of Exchange 2010 EMS

sends commands from the local PowerShell interpreter through WinRM, even when you're executing commands on the very same machine.

When you open an EMS window, you're actually creating a PowerShell *runspace,* into which the EMS command set is loaded. Your local runspace is what backs the EMS window that you see. There's also a corresponding runspace on the Exchange server that you're talking to. Even if you're running EMS on the Exchange server itself, you'll still have two runspaces. The object that links the two runspaces is known as a *session.* If you think of a Telnet or Secure Shell (SSH) session, you'll have an idea of what a PowerShell session is, with a twist: Telnet and SSH pass text back and forth; a PowerShell session sends binary data blocks that represent system objects back and forth. The PowerShell session is actually passed over the network via IIS.

This implementation offers a lot of benefits. For one, it makes the process of sending commands to remote machines transparent. Its implementation is tied into IIS, which means that IIS authentication and authorization can be used to control who can do what, which in turn enables the use of Role Based Access Control (RBAC), another key Exchange 2010 feature.

RBAC

The reason you can run Exchange commands in EMS is that when you launch the PowerShell interpreter, the Exchange command set is automatically loaded. In Exchange 2007, all the Exchange commands are loaded, meaning that any administrator can run any command. RBAC gives us a much more granular system of control. You can assign permissions to individuals or groups so that they can run only the commands you specify. In fact, you can control which parameters of those commands they can supply. For example, you could enable a group of Help desk technicians to use the Set-Mailbox cmdlet while giving them access to only some parameters rather than all of them.

This is possible because the RBAC permissions that you set are used to control which EMS cmdlets are loaded. If a user doesn't have permission to load a particular cmdlet, he or she can't execute that cmdlet. This means the user can't use functions in EMC or ECP that depend on that cmdlet. Both EMC and ECP are RBAC-aware, so they automatically hide things that the user can't do in the UI.

From a practical standpoint, you need to be aware of how RBAC permissions, roles, role assignments, and scopes work, because if any of them are set to deny users access to a particular cmdlet, the users won't be able to run the cmdlet. (For more information about RBAC, see "Exchange Server 2010 Role Based Access Control," April 2011, InstantDoc ID 129219.)

New EMS 2010 Features

In addition to the changed architecture, the EMS 2010 shell has several interesting new features compared with Exchange 2007. (Some of these features are actually included in SP1; however, I'll lump the release to manufacturing—RTM—and SP1 features together.)

New cmdlets for importing and exporting mailbox contents and PST files. In Exchange 2007, you could perform some limited manipulation of mailbox contents, but you had to have a 64-bit version of Microsoft Outlook installed on the server. In Exchange 2010 SP1, we now have the *-MailboxExportRequest and *-MailboxImportRequest cmdlet families. These cmdlets let you create mailbox import or export requests; these requests are analogous to the mailbox move requests you might already be familiar with.

When you create a request to export or import content, the Mailbox Replication Service (MRS) takes care of scheduling and processing the request. To export content, you use New-MailboxExportRequest to specify what mailboxes you want to export content from, which items should be exported, and where the results should go; the corresponding New-MailboxImportRequest lets you control how PST files are ingested and their contents stored in mailboxes. Note that you must specify the location of the PST files you want to import; Exchange doesn't currently include a way to search for PSTs on the network.

There are also cmdlets for getting the status of import or export requests. Microsoft's PST Capture tool (blogs.technet.com/b/exchange/archive/2011/07/05/coming-soon-pst-capture-tool.aspx) leverages these cmdlets to do some of its work, and you can combine these cmdlets with the multi-mailbox search functionality included in Exchange 2010 to find and archive the messages you're interested in.

Administrator audit logging. A common request (sometimes more of a plea, actually) from administrators is to find out who changed something or when it was changed. Exchange 2010 offers an administrator audit logging feature that does exactly this. When this feature is enabled, every cmdlet on the auditing list is audited and the audit results are stored in a hidden arbitration mailbox that you can search with the Search-AdminAuditLog and New-AdminAuditLogSearch cmdlets, so you can see who ran a cmdlet, when, where, and what the results were. Interestingly, you can only add cmdlets that change things (e.g., the Set-* family) to the auditing list; you can see who changed things but not who looked at things using the Get-* cmdlets. For more information about how audit logging works and how to take advantage of it, see the Microsoft TechNet article "Overview of Administrator Audit Logging" at technet.microsoft.com/en-us/library/dd335052.aspx.

A set of cmdlets, called *-MailboxFolderPermissions, for managing permissions on mailboxes and mailbox folders. These cmdlets make it ridiculously easy to do things such as give calendar reviewer permission to every user or find all users who have particular permissions. (For a clear example of how to write a useful script using these cmdlets, see Jan Egil Ring's Set-CalendarPermissions script at gallery.technet.microsoft.com/ScriptCenter/19b98a56-42aa-4695-b07c-335d8322b64e.)

The Send-MailMessage cmdlet. This cmdlet does just what its name suggests. You can use it to spam your friends, but it's more useful as a means to send status or warning email messages for tasks such as automatically notifying users whose passwords are about to expire, sending welcome email messages to new users, and so on.

The EMC cmdlet log. Technically, this might not be an EMS feature—but it's still useful. EMC 2010 can maintain and display a log of all the cmdlets that ran during an EMS session. This is a great way for you to keep track of what you did while

fixing a problem or to get a head start on automating a frequently needed set of commands. Auditing only records cmdlets that make changes, whereas the cmdlet log preserves every action taken in the session. To enable the log, use the View command in EMS's action pane, then select View Windows PowerShell Command Log; when the log appears, select Action, Start Command Logging. All the cmdlets you ran will appear in the log window. The log is retained only until you quit EMC, although you can export it to a file if you want to save it.

Other features. In addition to the other new bells and whistles, there are new cmdlets for working with the new features introduced in Exchange 2010—including cmdlets for creating and managing federation trusts, database availability groups (DAGs), Outlook Web App (OWA) mailbox policies, Exchange ActiveSync allow/block/quarantine lists, and other constructs that are new to Exchange 2010. One of the beautiful things about PowerShell in general is that if you can think of an object name, you can probably figure out what cmdlets apply to it. For example, if you know there's such a thing as an OWA mailbox policy, it doesn't take a lot of imagination to figure out that you'd create one with New-OwaMailboxPolicy or remove one with Remove-OwaMailboxPolicy.

Office 365

One very cool aspect of Exchange 2010 PowerShell that many administrators haven't run into yet is its ability to connect directly to Microsoft Office 365. This makes perfect sense when you think about it, given that Office 365 and Exchange 2010 run essentially the same PowerShell bits. However, the ability to seamlessly manage a hybrid Exchange organization using PowerShell is both very useful and technically slick.

To accomplish this task, all you need to do is create a PowerShell session that points to a specific URL at the Office 365 service. Because of the way the EMS uses WinRM, which in turn plugs into Microsoft IIS, it's simple to set up a connection by using code such as the following:

```
$creds = Get-Credential
$s = New-PSSession
  -ConfigurationName Microsoft.Exchange
  -ConnectionUri
    https://ps.outlook.com/powershell
  -Credential $creds
  -Authentication Basic
    -AllowRedirection
$importresults = Import-PSSession $s
```

This code looks more complicated than it is. The first line obtains your administrative credentials and stores them securely in a PowerShell credential object. The second line (which is actually shown here on multiple lines, for fit) establishes a new PowerShell session that connects to a remote endpoint. The third line attaches the Office 365 session to your local PowerShell session—it links your local session with the remote runspace. After completing these steps, you can issue partial commands that will be sent remotely to the Office 365 servers that host your mailboxes. Of course, you might not be able to do everything you can do with your on-premises Exchange servers: Microsoft has applied RBAC permissions to restrict what administrators can do, as well as what you can do. There doesn't seem to be a published guide that details exactly which commands are enabled for which roles, so it might require some experimentation. However, you'll probably find that most of the commands you have access to are related to recipient management and setting configuration parameters on mailboxes; don't expect to have access to cmdlets that control mailbox servers, Client Access servers, and other aspects of the environment that belong to the service provider.

An EMS 2010 Annoyance

One circumstance that often trips up administrators who are making the transition from Exchange 2007 to Exchange 2010 is that EMS 2010 handles object pipelines a bit differently. You'll recall that PowerShell collects sets of objects into pipelines for efficient, linear processing; the first object in a given pipeline is the first one evaluated, then the second, and so on. In Exchange 2007, pipelines are always local. In Exchange 2010, they're not. That's fine as long as you're trying to execute only one pipeline at a time. As soon as you do something that has the potential to generate multiple pipelines, you'll get an error that, rather unhelpfully, says, "Pipeline not executed because a pipeline is already executing. Pipelines cannot be executed concurrently."

The simplest way to fix this problem is to reduce the pipeline stage count. Instead of taking the output of one command and piping it directly to another, use an intermediate variable to separate the two. For example, instead of using Get-Mailbox and piping it directly to the *foreach* object or *where* object, you can get the output of Get-Mailbox, store it, and then pass it on like this:

```
$mailboxes = Get-Mailbox
$mailboxes | foreach { doSomething }
```

In this case, first we collect all the mailboxes into a single object, then we unpack that object—which is really a pipeline—and pass it through the *foreach* cmdlet so that we can perform the doSomething action on each object. This command involves a bit more typing, but it eliminates the additional pipeline stage that causes the concurrency error.

Moving Ahead

If you're familiar with EMS in Exchange 2007, you already know about 90 percent of what you need to manage Exchange 2010 effectively. As you learn more about the new Exchange 2010 features, you're already well-equipped to manage them with EMS 2010. If you're coming directly to Exchange 2010 from an older version of Exchange, you'll find that most of the material that covers EMS 2007 is still useful as an introduction. (For a list of applicable resources, see the online Learning Path.) Learning how to use PowerShell effectively is a key aspect of becoming comfortable with Exchange 2010, and this trend will only continue in future Microsoft releases as additional products embrace the use of PowerShell for management and control.

InstantDoc ID 140284

Paul Robichaux
(probichaux@windowsitpro.com) is a senior contributing editor for *Windows IT Pro*, a content author at Acuitus, and a Microsoft Exchange Server MVP and MCSE. Paul is the author of *Exchange Server Cookbook* (O'Reilly and Associates) and blogs at paulrobichaux.wordpress.com.

System Center Operations Manager

REPORTING TIPS

Make the most of this powerful and flexible reporting infrastructure

by Cameron Fuller

One of Microsoft System Center Operations Manager 2007's most powerful functions is its reporting functionality. Operations Manager reports are built on a data warehouse that's designed to gather raw data. Over time, this raw data is aggregated and only the aggregated data is retained for historical reports. This approach allows Operations Manager to store data for a long period of time without increasing the size of the data warehouse to such a level that reports take too long to run. Operations Manager uses SQL Server to store the data and SQL Server Reporting Services (SSRS) to provide the reporting functionality. Operations Manager provides the necessary framework for an extremely powerful reporting feature, including the ability to provide long-term historical trending reports.

Although Operations Manager's reporting structure is extremely powerful and flexible, it's also unintuitive and can be difficult to work with. This article provides 10 tips to help you make the most of your Operations Manager reporting environment. These tips focus on the following areas:

- Running reports in Operations Manager
- Finding reports for Operations Manager
- Generating your own reports in Operations Manager
- Integrating reports in Operations Manager

Running Reports

The most common complaint about Operations Manager reporting is how difficult it is to identify what object you need to run a report on. Running reports in Operations Manager isn't as simple as selecting objects from the screen and then running the report. It isn't uncommon to open a report, select what appears to be the appropriate object, run the report, and get a blank report. For example, you can't select a group of servers and run a free disk space report on them. If you're frustrated with getting blank Operations Manager reports, see the first five tips for information about how to find valid objects when running reports.

For an explanation of why a report is blank, we need to look at how Operations Manager functions. It uses an approach that takes different entities, referred to as objects, and defines a model for each object's heath. (For a full introduction to Operations Manager, see "Operations Manager Key Performance Indicators," January 2011, InstantDoc ID 128969.) Examples of Operations Manager objects include servers, processors, disks, and distributed applications such as Microsoft Exchange Server. Objects exist in a hierarchy such that a disk object is part of a server object. The objects can each have a defined health state, and they each have data that's used for reporting, as long as the performance counter is associated to the object. For example, if you choose a drive on a server as an object, you won't have a processor performance counter associated with it. If, however, you choose a computer object and the objects in it, you'll be able to see a processor performance counter.

Tip #1: Filter Options. In the original Operations Manager 2007 release, finding the correct object to choose for a report is often extremely difficult because the list of objects isn't restricted to objects that actually have data for the report. To select the appropriate object, you need to filter through all the available objects to find the correct one that has the data needed for the report. If you select the incorrect object and run a report, it will return no data. To address this issue, Microsoft added the Filter Options search feature in System Center Operations Manager 2007 R2. Several of Operations Manager 2007 R2's new reports are designed to show pre-filtered objects that have data for the report. If you click Search, you can see the objects that contain data for the report. This option doesn't exist for all reports—only reports that were rewritten in Operations Manager 2007 R2 to include the Filter Options feature.

To find reports in which the Filter Options feature is available, open the Reporting pane in the Operations Manager console and open a folder with reports. Open the report, then add an object. If the filter options are available for the report, you'll see the *Filter Options have been applied* message. A good example of Filter Options is available in the SQL Server Management Pack, in the user activity report.

The Service Level Tracking Summary report doesn't show the Filter Options, but when objects are added (shown as Service Levels), only acceptable objects (objects that have data for the report) are returned by the search. In my environment, I configured Service Level Tracking for the Operations Manager distributed application based on better than 99-percent availability. I also created my own line of business (LOB) application called LOB01 and configured Service Level Tracking based on better than 98-percent availability. If I add an object to the report, the Operations Manager distributed application and my LOB01 application will be listed for this report.

Tip #2: Reports with predefined objects. After working with Operations Manager reporting for a while, you might assume that to run a report, you must know the object that you want to run the report for. However, if you need to run a report in Operations Manager, don't assume that you need to select the correct object to run the report. Many reports have filter options available, and many of the reports included in Microsoft's management packs don't prompt for objects. Some examples of reports that don't prompt for objects include the following:

- Client Monitoring Views (Top N Applications, Top N Applications Growth and Resolution, Top N Error Groups, Top N Error Groups And Resolution)
- Microsoft Data Warehouse (Data Warehouse Properties)
- Microsoft Generic Report Library (Licenses, Most Common Alerts, Overrides)
- Operational Data Reporting Management Pack (Alerts Per Day, Instance Space, Management Group, Management Packs, Most Common Alerts)
- SCC Health Check Reports (which I discuss in more detail later)
- SQL Server 20008 Monitoring (Top 5 Deadlocked Databases)
- System Center Core Monitoring Reports (Agent Counts by Date Management Group and Version, Data Volume by Management Pack, Data Volume by Workflow and Instance)

These reports can be run through the Reporting pane without needing to select the appropriate object for the report, because objects are predefined.

Tip #3: Reports that document their objects with data. The Filter Options tip works well for reports that have this option available—however, this option isn't available in many reports. For such reports, highlight the report and check the report details, where you can often find a list of objects the report is looking for.

Figure 1 shows an example Windows Server Internet Information Services (IIS) 2003 report. Highlighted on this report is the list of objects that have data for the report. This example shows that objects with data for the report include IIS 2003 Web Server and IIS 2003 Role. This information isn't available after you run the report. Therefore, you need to check the reporting details in the Reporting pane before you run a report, to identify which objects will have data for the report. This information will make it much easier to locate the appropriate object for a report.

Tip #4: Running reports from the Monitoring pane. Up to this point, we've discussed tips to use in the Operations Manager console's Reporting pane. However, the best approach to running reports in Operations Manager is through the Monitoring pane. This is because of how Operations Manager uses objects. Objects have associated properties that indicate which reports are relevant. The Monitoring pane displays reports and tasks that are relevant to the highlighted object. Running reports from the Monitoring pane lets you avoid the requirement to select objects for a report.

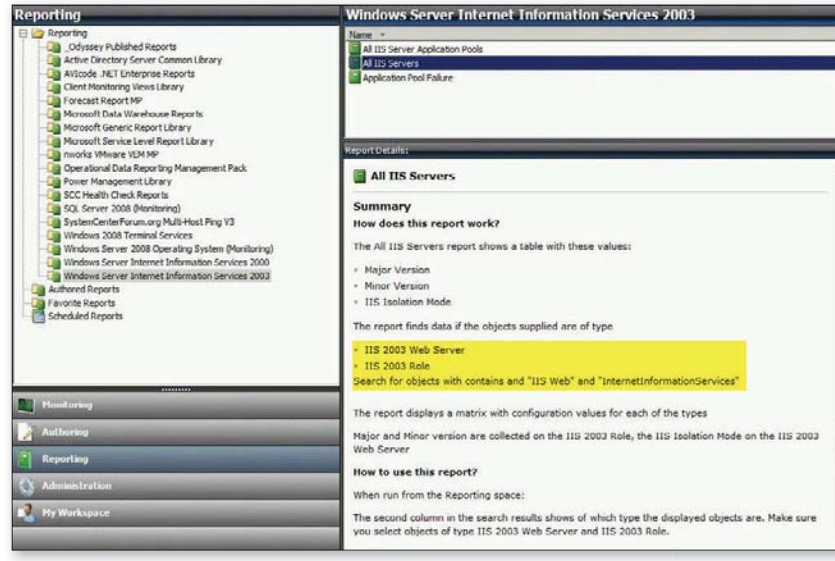


Figure 1: Checking a report's details to see objects that have data for the report

Selecting the Logical Disk State view in the Microsoft Windows Server folder and highlighting a drive in this folder lets you see various available tasks (e.g., Logical Disk Defragmentation, Run Chkdsk, Run Chkntfs, Start Computer Management Console, Volume Information). You can also see a variety of reports (e.g., Alert Logging Latency, Alerts, Availability, Configuration Changes, Disk Performance Analysis, Event Analysis, Health, Operating System Storage Configuration). If you run one of these reports, the highlighted object is passed to the report and you don't need to identify the appropriate object.

Because Operations Manager is built around this concept, the same approach works in the various Operations Manager console views, such as Alert View, Diagram View, Event View, or State View. (These views can be seen by right-clicking an object and selecting Open.)

Don't just assume that your reports must be run through the Reporting pane. Using the Monitoring pane to run reports lets you avoid challenges with identifying the appropriate objects and getting blank reports as a result.

Tip #5: Using a state view to run reports. Although the Monitoring pane provides the ability to pass objects to reports, it's often difficult to determine which specific view is needed to find the required objects. Management packs are stored in the Monitoring pane, in a folder structure that can be extremely complex. To simplify this approach, you can copy existing state views or create new state views and put them in a folder that's specifically designed to run reports from.

Create a new management pack in the Authoring pane (select Administration, Management Packs, then right-click and select Create Management Pack, QuickReports). After a management pack is created, it automatically creates a top-level folder in the Monitoring pane with the management pack name (e.g., QuickReports).

As an example, you can open the Microsoft Windows Active Directory folder, copy the DC State view, and paste it into the QuickReports folder. The DC State view can now also be renamed to make the view name more intuitive (e.g., "Active Directory," as Figure 2 shows). You can also create your own state views in this folder by opening the folder; right-clicking; selecting New, State View; and selecting the object.

Creating different state views for the required objects for a report lets you quickly select multiple objects (as many as 10 by default) and run the report. When you run a report in this manner, the objects that you select are passed to the report. For more information about using state views to run reports, see "QuickTricks: Creating really easy multiple server performance reports & how to create a report for multiple objects when you don't know what object(s) to choose" at tinyurl.com/2ar5hcy and "A Practical Example of the OpsMgr 'QuickReports' approach" at tinyurl.com/6xuc632.

Note that there's a registry entry for setting how many objects can be selected to run a task or report on. To change this value, start a registry editor and navigate to HKEY_CURRENT_USER\Software\Microsoft\Microsoft Operations Manager\3.0\Console\TaskSelectedObjectsLimit. Set the DWORD value to the following:

- -1 (xFFFFFF): Unlimited number of objects (not recommended)
- > 0: Maximum number of simultaneously selected objects for which tasks or reports will be generated; the default value is 10

The value can be changed, but this operation is considered "do at your own risk." As a general rule, you should leave the registry setting at a value of 10 unless there's a specific need to increase it for your environment. I've increased the value to 100, which lets me select as many as 100 objects for a report or a task, without any problems. In most cases, the value shouldn't exceed the number of servers in your environment. For more information about console-related registry keys, see "OpsMgr 2007: Registry keys to control the refresh of the admin console" at tinyurl.com/6elgwv3.

Finding Reports

The first five tips provide methods for using existing Operations Manager reports more easily. The next two tips assist with adding more pre-built reports into your Operations Manager environment and thus avoiding having to create your own reports.

Tip #6: Getting new reports from Microsoft. In Operations Manager, Microsoft includes reports within management packs. The ability to add management packs directly through the Operations Manager console was added in Operations Manager 2007 R2. In the Administration pane, under Management Packs, there are options to import or download management packs that you can add from the built-in Microsoft online catalog. This functionality helps you determine which of your management packs have updated versions available.

You can also use Operations Manager 2007 R2's Operations Manager console to easily determine which management packs are available but not yet installed. Installing the management packs for the technologies

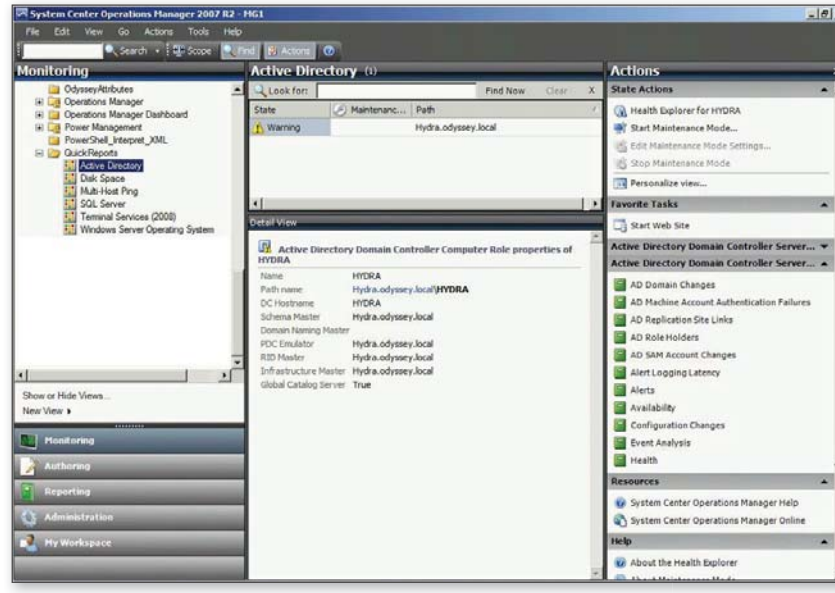


Figure 2: Creating a QuickReports folder to run reports from the Monitoring pane

that are relevant to your environment adds not only monitoring but also reporting functionality for these technologies.

The Microsoft System Center Marketplace (available at pinpoint.microsoft.com/en-US/systemcenter; formerly known as Pinpoint) provides a single location to find applications, professional services, and IT organizations. The System Center Marketplace website also provides the ability to download management packs for Operations Manager. This is especially useful in situations in which users can't connect to the Internet from the Operations Manager console, or when management packs aren't available in the Operations Manager console.

If the Report pane doesn't show the System Center Core Monitoring Reports in your environment, be aware that these reports aren't available if you upgrade existing management packs through the Operations Manager console. These reports are available from the System Center Marketplace. Alternatively, you can search the built-in Microsoft online catalog for available management packs and add System Center Core Monitoring Reports.

Many of Microsoft's recently released pre-built reports are extremely useful out of the box. For example, the Microsoft Data Warehouse report entitled Data Warehouse Properties can be used to show the current data warehouse size, as well as estimate sizing if the data retention periods are increased. (For more information, see "Changing the OpsMgr Data Warehouse retention periods & Using reports to assess impacts to Data Warehouse sizing" at tinyurl.com/6yo3r6o.)

In the most recent release of the Operations Manager management packs, Microsoft added new report designs that are more intuitive and that integrate historical information. Figure 3 shows the performance of a single system for processor, memory, disk, and network metrics.

This management pack also contains a report that displays Key Performance Indicators (KPIs) on a group of systems and their health, as Figure 4 shows. This report provides an easy way to compare performance for all servers in a web farm. For a custom LOB application, this report provides an intuitive way to report KPIs for all servers used in the application. These improved reports provide the ability to display a server's or group of servers' performance metrics and health in an extremely detailed and intuitive report.

Integrating the management packs that are relevant to your environment, as well as updating to the current versions of management packs, results in extremely useful pre-built Operations Manager reports.

Tip #7: Getting new reports from the community. The System Center community has stepped up, with many people creating and sharing reports. One of the best recent examples is the SCC Health Check Reports, released by System Center Central (www.systemcentercentral.com). None of the reports in this management pack prompt for objects (see Tip #2):

- Agents - Agent Hotfix Report (OM)
- Agents - Agents Missing Hotfix Report (OM)
- Agents - Down Agents (OM)
- Alerts - Alerts Closed by Specific User (DW)
- Alerts - Alerts Closed by User [Count] (DW)
- Alerts - Alerts Closed by UserID (DW)
- Alerts - Number of Alerts per Day (OM)
- Alerts - Top 20 Alerts By Alert Count (OM)
- Alerts - Top 20 Alerts By Repeat Count (OM)
- Config Churn - Discoveries Last 24 Hours (DW)
- Config Churn - Modified Properties Details Last 24 Hours (DW)
- Events - All Events Count By Last 7 Days (OM)
- Events - Most Common Events by Number and Publisher (OM)
- Events - Top 20 Computers Generating the Most Events (OM)
- Misc - Groups Report (OM)
- Misc - Infrastructure Overview (OM)
- Misc - Management Packs (OM)
- Misc - Operational and Datawarehouse Usage Report (OM) - (DW)
- Misc - Outage and Maintenance Report (DW)

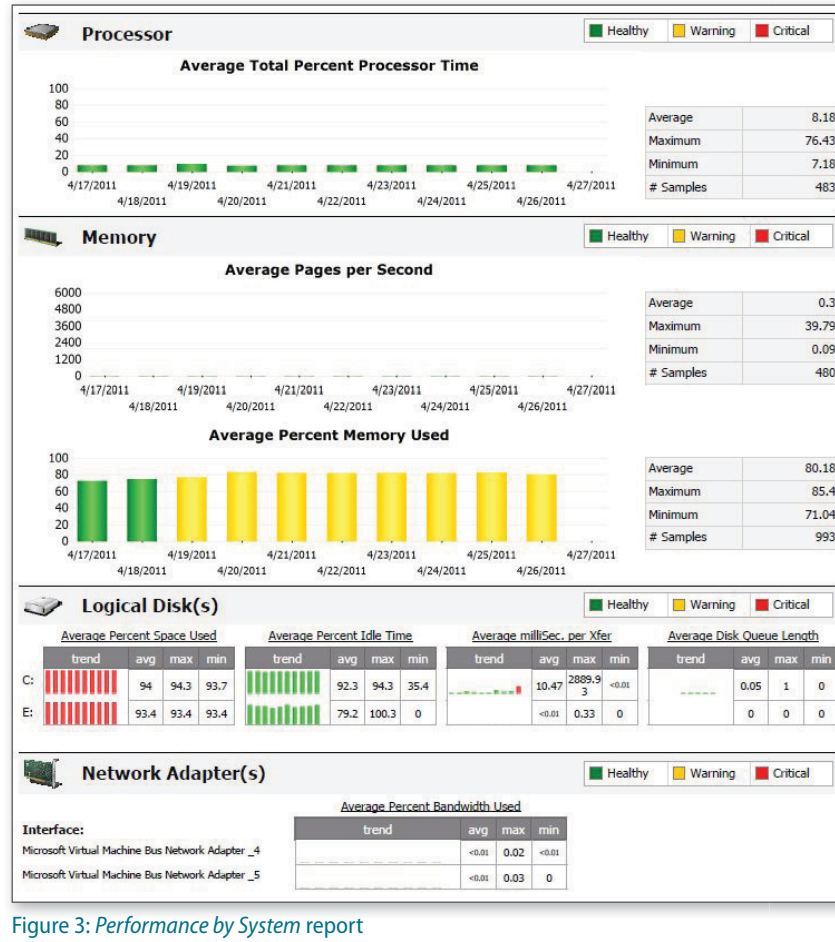


Figure 3: *Performance by System* report

Figure 4: *Performance by Utilization* report

- Misc - Run As Profiles (OM)
- Performance - Performance Inserts Per Day (OM)
- Performance - Top 20 Computers By Perf Count (OM)
- Performance - Top 20 Performance Insertions By Perf (OM)
- Performance - Top Performance Baseline Generating Rules (OM)
- State - Noisiest Monitors (OM)
- State - Old State Changes Not Groomed (OM)
- State - State Changes Per Day (OM)

This management pack is available for free from System Center Central, in the management pack catalog (tinyurl .com/5wscr5e).

Another example of an extremely useful community-written management pack is Daniel Savage's forecasting report (tinyurl .com/6jnzsxt). This report lets you use an existing performance counter gathered by Operations Manager and forecast for a period of time based on the historical data provided by the performance counter.

Both Microsoft and the System Center community have been continuing to develop and share new reports since Operations Manager was released. Before developing your own reports, review what's already available to see if someone else has already created what you need for your environment.

Generating Your Own Reports

Despite the number of reports available for Operations Manager (hundreds, depending on which management packs are installed in your environment), there are situations in which a preexisting report won't meet your reporting requirements. A variety of methods are available for creating your own reports, including creating linked reports or using Report Builder or Visual Studio. For more information about creating custom reports, consult *System Center Operations Manager 2007 Unleashed* (Sams, 2008; tinyurl.com/27mqnm) or "Operations Manager 2007 Management Pack and Report Authoring Resources" (tinyurl .com/6h2n335).

Tip #8: Using the performance view to generate new reports. A common approach to creating reports is to use the Microsoft Generic Report Library. This library was designed to provide a flexible method for configuring reports to meet custom business requirements. The most commonly used generic report is the Microsoft Generic Report Library's performance report. The challenge with using this report is the same one I discussed in the first five tips in this article: How do you know what object (or other information) is needed? Let's consider the most commonly asked question in generic report creation: "How do I create a free disk report for multiple objects?" There's currently no pre-built report that covers this topic—so, how do you create one?

Instead of going directly to the Reporting pane, open a performance view in the Monitoring pane. To see a larger view of the data, open the performance view in a new window. From this view, look for items by using the text search option on the % Free Space counter. From the performance view, you can see all the information that's needed to customize the generic performance report. As Figure 5 shows, most of the fields in the performance view match the fields required when creating a generic report:

- Path
- Rule
- Counter
- Instance

The following two field names need to be mapped to a different name when creating the report:

- "Target" = "Object" when customizing the report
- "Object" = "Performance object" when customizing the report

The performance view provides a quick way to identify the values that should be used when customizing this generic report. Gathering the appropriate counters ahead of time in this view and taking a screenshot can significantly decrease the complexity in customizing this report. For step-by-step details on how to create a free disk space report, see "Creating Useful Custom Reports in OpsMgr: How to create a simple free disk space report" at tinyurl .com/23azujx.

Report Integration

The ability to run ad-hoc reports isn't the only reporting function available in

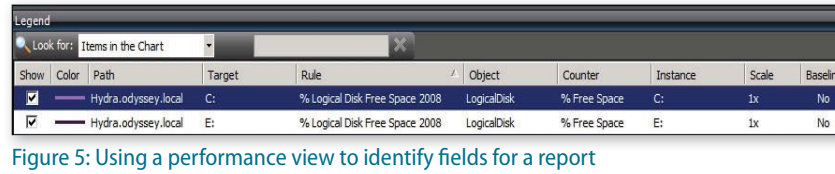


Figure 5: Using a performance view to identify fields for a report

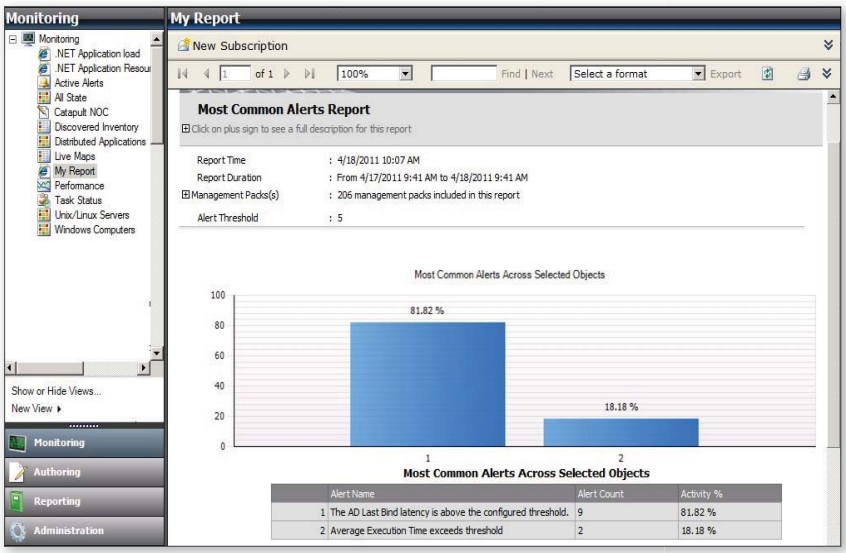


Figure 6: Displaying a report in the Monitoring pane

Operations Manager. You can also use SSRS's functionality to schedule and deliver reports.

Tip #9: Scheduling and delivering reports. Operations Manager reporting gains additional functional benefits from being built on SSRS. The previous tips in this article focused on using the reporting functionality to run ad-hoc reports; Operations Manager can also schedule report creation and delivery. Operations Manager reports can be scheduled for delivery to a file share or sent via email.

Reports can be generated using multiple formats (e.g., Microsoft Excel, RPL Renderer, Microsoft Word, Adobe PDF, Tiff, MHTML, CSV, HTML 4.0, XML). These files can be stored in a folder structure to provide historical copies or the most recent execution of a report.

Emailing reports is commonly used to provide weekly (or daily) information focused to a specific group of users, providing performance information for their servers. For example, application owners might want to receive weekly performance reports for all servers in a web farm, or Operations Manager administrators might want to receive daily reports of all agents that are currently down—for example, SCC Health Check Reports: Agents - Down Agents (OM).

The ability to schedule Operations Manager report generation and delivery is very useful. Although this functionality is built in to SSRS, it's often overlooked in Operations Manager environments.

Tip #10: Integrating reports into dashboards and the Operations Manager console. In "Operations Manager Dashboards" (February 2011, InstantDoc ID 129233), I discuss dashboard options that are available for Operations Manager. One of these options uses the Service Manager dashboard to provide Operations Manager dashboard functionality. The Service Manager dashboard is built on Microsoft Office SharePoint Server, which provides additional flexibility, such as including another website within a web part (the Page Viewer Web Part). Reports in Operations Manager are accessible via a URL, so integration of reports is simple when you know the URL to add to the dashboard.

To identify the URL to use to access a report, do the following:

1. In the Operations Manager console's Reporting pane, configure the report as you'd like it to display.
2. After configuring the report, use the File/Publish option.
3. From the Operations Manager console, select Administration, Settings, Reporting to identify the URL of the reporting site.
4. Browse to the specified server (http://<servername>/reports). Open the My Reports folder, then open the report you published. Copy the URL from the top of the web page.

Dashboard integration can include the actual report in the Page Viewer Web Part or can provide a link that can be used to expand on information shown in the dashboard. For example, you can provide a link for the Operations Manager dashboard that gives details on the most common alerts in an environment.

In addition, you can use a link that expands on an item shown in the dashboard. You can create a dashboard that displays the amount of time it's currently taking to execute a synthetic transaction on a website. From this dashboard, you can include a link to a report that provides historical trends for the same synthetic transaction. The key idea is that URLs are available and can be integrated into a variety of dashboard solutions to provide a more comprehensive experience for dashboard users.

The Operations Manager console also has a view called the Web Page View. This view is available in the Monitoring pane and provides the ability to display a URL in the Operations Manager console. Using the path for the report that you identified in Step 4, you can integrate the URL so that it's visible in the Operations Manager console, as Figure 6 shows.

Something to be aware of when transferring URLs for reports into the Web Page View is that the reporting URL uses a value of %2f to represent the / (slash) character. The Web Page View doesn't accept these characters; to get the view to display the web page, you need to substitute %2f with / (slash).

Harness the Power

Operations Manager's reporting functionality is extremely powerful but often underutilized. Using the 10 tips in this article can help make the most out of your Operations Manager reporting environment and can provide a more comprehensive solution for your Operations Manager users and administrators.

InstantDoc ID 140603

Cameron Fuller
(cameron.fuller@catapultsystems.com) is a principal consultant for Catapult Systems, an IT consulting company and Microsoft Gold Certified Partner. He's an Operations Manager MVP and co-author of *System Center Operations Manager 2007 R2 Unleashed* (Sams) and *System Center Operations Manager 2007 Unleashed* (Sams).

FEATURE

Renaming Scheduled Tasks in Windows 7, Server 2008, and Vista

This PowerShell script lets you overcome a Task Scheduler limitation

by Bill Stewart

The Task Scheduler service in Windows is a very useful automation tool. Starting with Windows Vista and Windows Server 2008, the Task Scheduler service got an overhaul. It has new trigger types, actions, and task folders. It also has a built-in scriptable object interface for managing scheduled tasks. (Microsoft provided a scriptable object interface for the Task Scheduler in earlier Windows versions, but it was a separate download.) Figure 1 shows the updated Task Scheduler window on a Windows 7 computer.

In Windows Server 2003, Windows XP, and Windows 2000, scheduled tasks are .job files found in the computer's \%SystemRoot%\Tasks folder. In these OS versions, renaming a task is easy: Press F2 when the task is highlighted in Windows Explorer or right-click the task in Task Scheduler and select Rename. In Windows 7, Vista, and Server 2008, Task Scheduler tasks are no longer stored as .job files in the Tasks folder, so you can't rename a scheduled task after you create it.

I don't know the reasons for the omission of this seemingly simple feature, but there is a workaround: Export the task as an XML file, import the task to create a new task with the new name, then delete the old task. This seemed like an unnecessary amount of extra work, so I wrote a PowerShell script, Rename-ScheduledTask.ps1, to make renaming a task easier.

You can download Rename-ScheduledTask.ps1 from the *Windows IT Pro* website. (Go to www.windowsitpro.com, enter 140368 in the Search box, and click the 140368.zip hotlink.) The script works on only Windows 7, Vista, and Server 2008 for two reasons. First, this script isn't needed in earlier OS versions. Second, the script object interface it uses isn't present in earlier OS versions. You can use the script to rename tasks on the local machine and remote computers. If you want to rename a task on the local computer, you must run the script from an elevated PowerShell window (i.e., right-click the PowerShell shortcut and choose *Run as administrator*).

How to Use the Script

The script's command-line syntax is as follows:

```
Rename ScheduledTask
  [TaskName] <String>
  [NewName] <String>
  [ComputerName <String>]
  [ConnectionCredential <PSCredential>]
  [TaskCredential <PSCredential>]
```

The only required parameters are -TaskName and -NewName, which you use to specify the task's current name and new name, respectively. Because the -TaskName and -NewName parameters

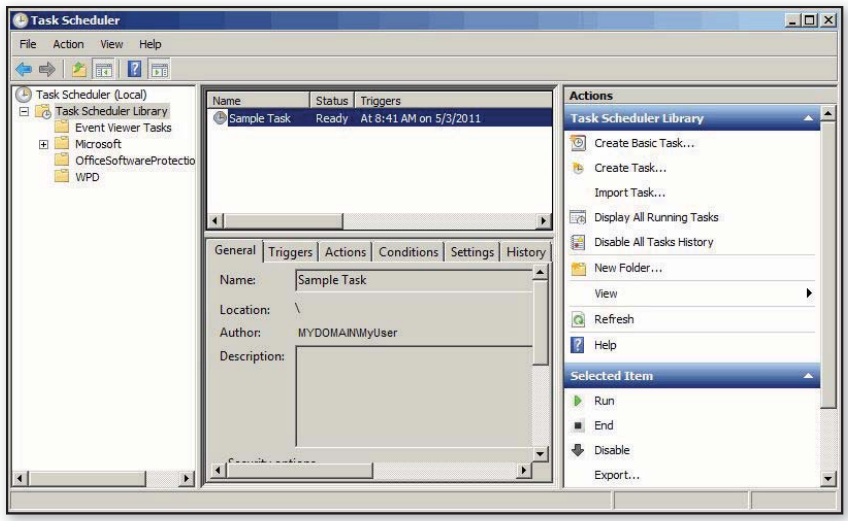


Figure 1: Windows 7 Task Scheduler

must be the first and second parameters on the script's command line, including the parameters' names (-TaskName and -NewName) is optional.

The overhauled Task Scheduler service supports task folders. If you specify a task name without a task folder name, the script assumes the task is in the root tasks folder ("\"). You can relocate a task to a different task folder by specifying the task folder's name as a part of the task's new name. The task folder will be created if it doesn't exist. For example, the command

```
Rename ScheduledTask
  "My Task"
  "\User Tasks\User Task 1"
```

renames the task named *\My Task* to *\User Tasks\User Task 1*. The \User Tasks folder will be created if it doesn't exist.

You use the -ComputerName parameter to specify the computer where the task to be renamed is stored. You can't move tasks between computers, so the renamed task will also be stored on that computer. If you omit the -ComputerName parameter, the script assumes the task to be renamed is on the current computer.

The -ConnectionCredential parameter specifies a PSCredential object for connecting to the Task Scheduler service on the computer (which is the local computer if you omit the -ComputerName parameter). Note that Rename-ScheduledTask.ps1 renames a task by copying the original task to a new task, then deleting the original task. This means that if the original task has saved credentials, they can't be copied because credentials are stored securely. So, before you use the -ConnectionCredential parameter, you should check the task's properties to see whether the task has saved credentials. As Figure 2 shows, when the *Run whether user is logged on or not* option is selected and the *Do not store password* option isn't selected, the credentials are saved. Thus, the credentials must be re-created when the new task is created.

If the original task has saved credentials, Rename-ScheduledTask.ps1 will prompt you for credentials when creating the copy. If you don't want the script to prompt you for credentials, you can include the -TaskCredential parameter, which requires a PSCredential object as its argument. (See the sidebar "Clarifying Credential Confusion" for more information about the -ConnectionCredential and -TaskCredential parameters.)

Aside from the inability to copy credentials, there is one other notable side-effect of copying a task: The new copy of the task won't have the original task's history of events, which appear on the History tab of the properties page. If the task's event history is important, save the task's history to a file before renaming it.

The script's online help provides a comprehensive list of sample commands. To view the sample commands, run the following code at a PowerShell prompt:

```
Get-Help Rename ScheduledTask -full |
  more
```

Inside the Script

Rename-ScheduledTask.ps1 uses the Schedule.Service programmatic identifier (ProgID) to create the TaskService object, which provides access to the Task Scheduler service for managing registered tasks. The TaskService object doesn't exist on Windows versions prior to Vista and Server 2008. See the "Task Scheduler Scripting Objects" web page (msdn.microsoft.com/en-us/library/aa383607

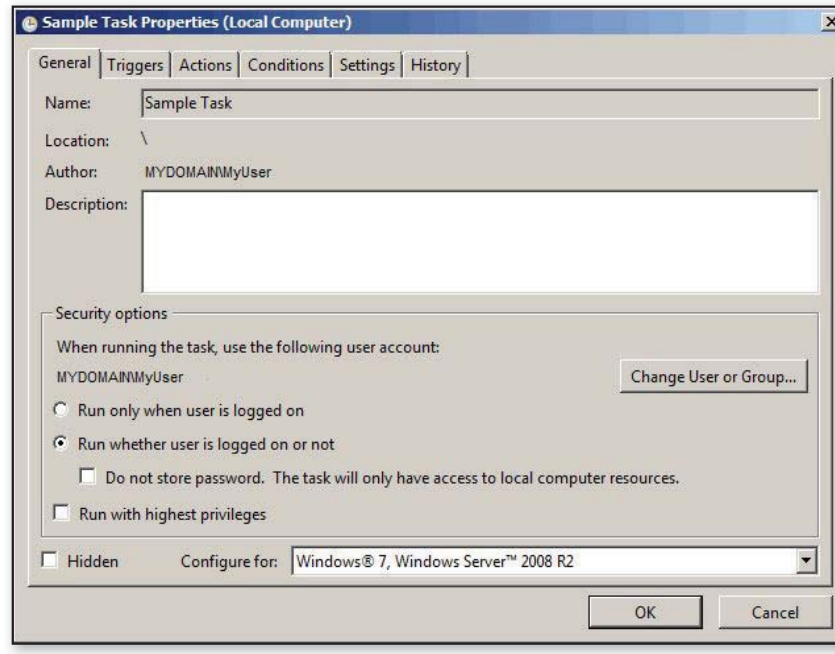


Figure 2: Task properties

Listing 1: The get-plaintextpwd Function

```
function get-plaintextpwd($credential) {
  $credential.GetNetworkCredential().Password
}
```

Listing 2: The get-taskname Function

```
function get-taskname($taskFolder) {
  $tasks = $taskFolder.GetTasks(0)
  $tasks | foreach-object { $_.Path }
  $taskFolders = $taskFolder.GetFolders(0)
  $taskFolders | foreach-object
       { get-taskname $_ }
}
```

.aspx) for more information about the TaskService object and its associated objects.

Next, the script uses the TaskService object's Connect method to try to connect to the Task Scheduler service. If the -ConnectionCredential parameter exists on the command line, the script uses the get-plaintextpwd function, shown in Listing 1, to return the PSCredential object's Password property as a plain-text string. The script does this because the TaskService object's Connect method doesn't support PSCredential objects.

After connecting to the Task Scheduler service, the script checks the HighestVersion property of the TaskService object. This property is a 32-bit unsigned integer that contains the internal version number of the Task Scheduler service. The most significant 16 bits represent the major version number, and the least significant 16 bits represent the minor version. Internally, the Task Scheduler version in Windows 7, Vista, and Server 2008 is 1.2 (65538), so the script checks that the HighestVersion property is at least this version before continuing. If the service's version is too old, the script throws an error and exits.

If the Task Scheduler service version is recent enough, the script uses the TaskService object's GetFolder method to get the root tasks folder. The script then uses the get-taskname function, shown in Listing 2, to retrieve a list of all task names from all task folders. It uses the list of task names to check the validity of the -TaskName and -NewName parameters.

Next, Rename-ScheduledTask.ps1 retrieves the TaskDefinition object for the task named with the -TaskName parameter. The TaskDefinition object defines all the components of the task. If the task has stored credentials, the script checks whether the -TaskCredential parameter was specified. If it wasn't specified, the script uses the Get-Credential cmdlet to prompt for credentials. (Canceling this prompt throws an error and ends the script.) If -TaskCredential was specified, the script uses the get-plaintextpwd function to convert the PSCredential object's Password property to plain text.

Finally, the script uses the RegisterTaskDefinition method to create a copy of the task. Note that if the task requires credentials but the supplied credentials aren't valid, the task won't be created and the script will throw an error. If the script creates the new task successfully, it uses the DeleteTask method of the original task's TaskFolder object to delete the original task.

Make the Rename Restriction Less Annoying

The overhauled Task Scheduler service includes many improvements over earlier versions, but the inability to rename a scheduled task is an annoying limitation. However, with the Rename-ScheduledTask.ps1 script in hand, it's a nuisance you're no longer forced to live with.

InstantDoc ID 140368

Clarifying Credential Confusion

There are two sets of credentials you might need when renaming a scheduled task using Rename-ScheduledTask.ps1:

- The -ConnectionCredential parameter specifies the credentials to use to connect to the schedule service on the computer where the task is stored (either the local computer or a remote computer). If you aren't a member of the Administrators group on the computer hosting the task, you can connect to the schedule service using administrator credentials.
- The -TaskCredential parameter specifies the credentials for the task itself, if needed. Task credentials are needed only when the task's *Run whether user is logged on or not option* is selected and the *Do not store password* option is not selected. If credentials are required and you don't specify the -TaskCredential parameter, the script will prompt you for credentials.

Both the -ConnectionCredential and -TaskCredential parameters require a PSCredential object as their argument. A PSCredential object securely stores a username and password for use in security operations. However, there is an important caveat you need to know about: Rename-ScheduledTask.ps1 converts the secure passwords in PSCredential objects to plain text because the scripting object model doesn't support PSCredential objects.

You can easily create PSCredential objects by using the Get-Credential cmdlet. Run the command

```
Get-Help Get-Credential
```

at a PowerShell prompt for more information about PSCredential objects.

InstantDoc ID 140575

Bill Stewart
(bstewart@iname.com) is a scripting guru who works in the IT infrastructure group at Emcore in Albuquerque, New Mexico. He has written numerous articles about Windows scripting and is a moderator for Microsoft's Scripting Guys forum. He has also written some useful free tools for the Windows IT community, which are available from his website at westmesatech.com.

Microsoft® SQL Server®
DENALI LAUNCH
CONFERENCE & EXPO

SPRING 2012 LAS VEGAS, NV

EXCHANGE MANAGEMENT SHELL
LYNC
OFFICE 365
WINDOWS INTUNE
VIRTUALIZATION
BI SEMANTIC MODEL
SYSTEM CENTER VIRTUAL MACHINE MANAGER
SYSTEM CENTER ORCHESTRATOR
SQL SERVER "DENALI"
SQL AZURE
EXCHANGE ONLINE
WINDOWS 8
SHAREPOINT
DAGs
WINDOWS SERVER 2008 R2 SP1

KEYNOTE SPEAKERS

QUENTIN CLARK
MICROSOFT
CORPORATE VICE PRESIDENT, DATABASE SYSTEMS GROUP, MICROSOFT SQL SERVER

SCOTT GUTHRIE
MICROSOFT
CORPORATE VICE PRESIDENT .NET DEVELOPER PLATFORM

STEVE FOX
MICROSOFT
DIRECTOR, DEVELOPER AND PLATFROM EVANGELISM FOR SHAREPOINT

JIM MCBEE
ITHICOS SOLUTIONS

MARK MINASI
MINASI RESEARCH AND DEVELOPMENT

MAR. 26 - 29, 2012
LAS VEGAS, NV
MGM GRAND

Be Here!

DevConnections and Microsoft will team up to launch the next version of SQL Server at MGM Grand in Las Vegas, Nevada.

powered by Microsoft® & SQL Server CONNECTIONS

CO-LOCATED WITH:

WINDOWS CONNECTIONS
Microsoft® Exchange CONNECTIONS
UNIFIED COMMUNICATIONS CONNECTIONS
SharePoint CONNECTIONS
Microsoft® Visual Studio CONNECTIONS
Microsoft® ASP.net CONNECTIONS
HTML5 CONNECTIONS
Windows Azure CONNECTIONS

REGISTER TODAY! www.WinConnections.com • 800.438.6720 • 203.400.6121

Backing Up SharePoint

Content, Configurations, and Components

What tools to use and how to use them

by Michael Noel

Backing up and restoring SharePoint 2010 databases, content, and configurations can be a complex endeavor. Microsoft has made some significant improvements to the native tools, including the addition of features that let administrators back up an entire farm configuration, an individual web application, an individual site collection, or even specific content. In addition, administrators can now connect to unattached content databases and restore content from them. With that said, it isn't immediately obvious which backup and restore tools are best for which situations and how to use them. So, I'll first shed some light on the available backup and restore tools, then concentrate on the tools with which administrators should be familiar.

Knowing Your Options

There is a wide array of options to back up a SharePoint environment:

- SQL Server tools. SharePoint content that's stored in SQL Server databases can be backed up using SQL Server's built-in backup and restore tools. You can initiate the backup as a one-time task or as a scheduled job. SharePoint database backups can be combined with other SharePoint backups, such as those available through SharePoint's Central Administration site or the SharePoint 2010 Management Shell. Unlike SharePoint restore procedures, SQL Server restore procedures can't restore item-level objects. Only complete database restores are possible.
- Central Administration tools. The Central Administration site includes several tools that can be used to backup and restore the SharePoint environment. However, not all backup and restore options are available when using the Central Administration tools.
- SharePoint 2010 Management Shell. SharePoint 2010 introduces the SharePoint 2010 Management Shell, which is built on top of Windows PowerShell. By executing SharePoint-specific PowerShell commands in the SharePoint 2010 Management Shell, administrators can gain some functionality that isn't available through the Central Administration tools.
- Recycle Bin. Originally introduced in the SharePoint 2007 wave of products, this tool is used by users and administrators. Data can be restored by users within 30 days of deletion and thereafter by site collection administrators. SharePoint 2010 SP1 added the Site Recycle Bin, which lets site collection administrators restore entire sites that have been deleted.
- AppCmd. Using the AppCmd command-line tool, administrators can back up the Internet Information Services (IIS) 7.0 configuration file on a Windows Server 2008 machine. The IIS 7.0 configuration file consists of web.config and applicationHost.config files. When a system failure

occurs, administrators can restore the IIS 7.0 configuration from the backup file.

- Stsadm. Although available in SharePoint 2010, Stsadm has been deprecated and is provided only to support backward compatibility. PowerShell is the preferred option—and in certain situations, the only option—for managing the SharePoint 2010 environment.
- Microsoft System Center Data Protection Manager (DPM) 2010. DPM 2010 is Microsoft's enterprise backup tool. It does snapshot-level backup and restore of SharePoint content, providing for full-farm or item-level recovery. DPM is a separate component that isn't included with SharePoint 2010.
- Third-party backup tools. Multiple vendors have backup tools for SharePoint 2010 that offer advanced functionality, such as item-level restores.

By using the SQL Server backup and restore tools and SharePoint 2010 Management Shell in addition to the backup and restore options in Central Administration, you can be fully prepared in the event of outages and other problems. Let's take a closer look at these three tool sets.

Using the SQL Server Tools

Fully loaded, a SharePoint 2010 environment will have about 25 databases that contain a significant amount of crucial content. (By *fully loaded,* I mean deployed with FAST Search Server 2010 for SharePoint; Microsoft Office Web Apps; all service applications; and content, logging, and configuration databases.) That's a huge number of databases to maintain and back up. To minimize the potential for lost content, it's crucial to have a solid database backup plan.

There are many options available to back up and restore SharePoint databases. In addition to the Central Administration tools and SharePoint 2010 Management Shell, other options include using SQL Server Management Studio (SSMS) or T-SQL scripts. You can also use a third-party database backup tool.

No matter which tool you use, it's important to understand that when you back up the databases, the search index and any web server customizations aren't backed up. So, database backups generally aren't the only backup option chosen by most administrators.

SQL Server offers many different types of database backups, including:

- Full backup. The entire database (including the transaction log) is backed up.
- Differential backup. All the data changes since the last full backup are recorded.
- Transaction log backup. All transactions performed against the database since the last full backup or the last transaction log backup are backed up.
- File and file group. A portion of the database is backed up.
- Partial backup. All data in the primary group, every read-write file group, and any specified files are backed up. File groups marked as read-only are skipped.
- Differential partial backup. Although similar to the partial backup, this backup only records changes to the data in the file groups since the previous partial backup.
- Copy-only backup. Unlike the other types of backups, a copy-only backup isn't recorded in the database and isn't used for restoration. Any type of backup (e.g., full, differential, partial) can be a copy-only backup.

Here's an example of how to use SSMS to perform a full backup:

1. Open SSMS.
2. In the Connect to Server dialog box, select the name of the database server you want to connect to and click Connect.
3. In the left pane of Object Explorer, expand the Server folder, then the Database folder.
4. Select the SharePoint database you want to back up.
5. Right-click the database, select Tasks, then click Back Up.
6. In the General page of the Back Up Database window shown in Web Figure 1 (www.windowsitpro.com, InstantDoc ID 140038), confirm the name of the database to be backed up and confirm that the *Backup type* option is set to Full.
7. Set the *Backup component* option to Database.
8. In the *Backup set* section, enter the name and description for the database backup.
9. In the Destination section, select Disk or Tape. (The Tape option will be grayed out if there are no tape devices attached to the database server.) You can back up information to as many as 64 disk devices or tape devices. If multiple devices are specified, the backup information will be spread across those devices. All the devices must be present to back up the database. If you need to add a device, click Add, enter the requested information, and click OK to return to the Back Up Database window.
10. Click Options in the *Select a page* pane to configure advanced backup options. (Alternatively, you can click OK to initiate the backup if you don't want to configure any advanced backup options.)
11. In the Options page's *Overwrite media* section, you can choose to add the backup to an existing media set or new media set. If you want to add the backup to the existing media set, you have the option of appending it to the existing backup set or overwriting all existing backup sets. For this example, maintain the default settings of *Back up to the existing media set* and *Append to the existing backup set.*
12. In the Options page's Reliability section, leave the *Verify backup when finished* option selected. Microsoft recommends that you leave it selected so that your database backup is verified. However, the verification process extends the time it takes to complete the database backup.
13. In the Options page's Reliability section, select *Perform checksum before writing to media.* This option ensures that the database backup is completed without any errors. However, the checksum process extends the time it takes to complete the database backup.
14. In the Options page's Reliability section, select *Continue on error.* This option ensures that the database backup will continue even if an error is encountered. However, selecting this option will have an impact on the performance of the server because it increases CPU overhead.
15. Click OK to execute the backup.
16. Review the backup operation's success or failure error messages and click OK to finalize.

17. Repeat steps 2 through 16 for any additional SharePoint databases.

Using the Central Administration Tools

The most obvious choice to back up SharePoint configurations and components is to use the built-in tools in the Central Administration site. The site's Backup and Restore page comes with two options: Farm Backup and Restore and Granular Backup. Using the Farm Backup and Restore option, administrators can back up and restore a complete farm, a farm's configuration, or individual components in a farm. New to SharePoint 2010, you can use the Granular Backup option to back up a site collection, export a document library or list, and recover data from an unattached content database.

As with previous versions, scheduling backups via the Central Administration site isn't an option. However, you can perform a one-time backup. For example, to back up a farm configuration, you need to perform the following steps:

1. Open the Central Administration site on a SharePoint server. Select All Programs on the Start menu, click Microsoft SharePoint 2010 Products, and choose SharePoint 2010 Central Administration.
2. Select Backup and Restore in the Quick Launch toolbar.
3. Select the *Perform a backup* option in the Farm Backup and Restore section.
4. In the Select Component to Back Up page, select the Farm component and click Next.
5. In the Select Backup Options page shown in Web Figure 2, select Full in the Backup Type section.
6. In the *Data to back up* section on the same page, select *Back up only configuration settings*.
7. In the *Backup location* text box on the same page, enter a backup location.
8. Click Start Backup.

After starting the backup, SharePoint 2010 displays the Backup and Restore Job Status page. It might take several minutes for the backup process to appear on the page, depending on the backup type and the data being backed up. It might be necessary to refresh the screen occasionally to see the updated status. You can also monitor the backup progress by clicking the View History link, which shows the historical backup progress rather than the current status.

You can view the backup files in the location you selected in step 7. You'll find an XML manifest and files with .bak extensions. The XML manifest is required for a restore, so don't delete it.

Restoring content is more difficult than backing up content. Fortunately, restoring content is fairly straightforward with the Central Administration tools. For example, here are the steps to take to restore a farm:

1. Create a new farm to which to apply the restore if it doesn't already exist.
2. Open the Central Administration site on a SharePoint server.
3. Select Backup and Restore in the Quick Launch toolbar.
4. Select the *Restore from a backup* option in the Farm Backup and Restore section.
5. In the Backup and Restore History page, enter where your backup files are located in the Backup Directory Location text box.
6. In the Top Component column, select the farm that you want to restore and click Next.
7. It will take a few minutes before the Select Component to Restore page appears. On this page, select the farm components you want to restore and click Next.
8. In the Select Restore Options page, select either the *New configuration* option or the *Same configuration* option. Choose the *New configuration* option if you want to restore the data to a farm with a different configuration, in which case it'll have different computer names, web application names, and database server names. Choose the *Same configuration* option if you want to restore the data to the same farm, in which it'll have the same computer names, web application names, and database server names.
9. Click Start Restore to commence the restore process.

Using the SharePoint 2010 Management Shell

The SharePoint 2010 Management Shell makes it easy to automate backup and restore processes. All the backup and restore options in the Central Administration site can be initiated in this tool. For example, to back up a farm configuration, you'd execute the following PowerShell command from the SharePoint 2010 Management Shell:

```
backup-spfarm -BackupMethod Full
  -Directory C:\Backup\
  -ConfigurationOnly
```

(Although this command wraps here, you'd enter it all on one line in the SharePoint 2010 Management Shell. The same holds true for the following command.) To back up a single web application, you'd execute this command:

```
backup-spfarm -BackupMethod Full
  -Directory C:\Backup\
  -Item http://webapplicationname
```

Besides automating backup and restore processes, administrators can schedule their backups—something not possible with the Central Administration tools. For more information about using PowerShell for SharePoint backup and recovery, see the "Backup and recovery cmdlets (SharePoint Foundation 2010)" web page at technet.microsoft.com/en-us/library/ee890117.aspx.

Developing a Backup Strategy

The wide array of tools to back up SharePoint content, configurations, and components can be quite daunting. However, you can develop a backup strategy that has the correct mix of tools based on your business requirements. A good place to start is to use the SQL Server tools and SharePoint 2010 Management Shell along with the backup and restore options in Central Administration. With these tools, you can effectively back up your SharePoint environment and restore it if needed, without any loss to your business.

InstantDoc ID 140038

Michael Noel
is a partner at Convergent Computing (www.cco.com), a Microsoft SharePoint MVP, and the author of books on SharePoint, Windows Server, ISA Server, and Exchange Server. His latest book is *SharePoint 2010 Unleashed* (Sams).

- TMS RamSan-810
- VMware Fusion/Workstation
- TITUS TMC
- Drobo B1200i

Texas Memory Systems RamSan-810 Delivers High Performance

Texas Memory Systems (TMS) announced its first enterprise MLC product, the RamSan-810, which brings Tier-0 performance and reliability to Tier-1 read-heavy workloads. The 10TB RamSan-810 has powerful 8Gb Fibre Channel or QDR InfiniBand interfaces and dissipates only 250W. Reliability of the RamSan-810 is enhanced by the TMS Series-7 Flash Controller (FPGA, PowerPC based), which utilizes an advanced error correction algorithm and patented Variable Stripe Raid (VSR) algorithm. The RamSan-810 is rated for a 10-year life with a 50TB/day write workload. For more information, visit www.ramsan.com/products/rackmount-flash-storage/ramsan-810.

Ensim Enhances Connector for SharePoint 2010

Ensim has significantly enhanced its SharePoint Manager, which provides provisioning, management automation, and compliance capabilities to Microsoft SharePoint Server 2010. Part of Ensim Unify Enterprise Edition's suite of integrated tools, SharePoint Manager supports both SharePoint 2007 and SharePoint 2010. Key enhancements for Ensim Unify SharePoint Manager are automated provisioning of SharePoint sites, including site collection and sub-sites; permissions management; and SharePoint group management. For more information, visit www.ensim.com/products/ensim_unify/unify_enterprise_edition/sharepoint_manager.html.

PRODUCT SPOTLIGHT

VMware Ships Fusion 4 and Workstation 8

VMware has updated two of its least expensive virtualization products, announcing that VMware Fusion 4 and VMware Workstation 8 are now shipping and available for purchase. VMware Fusion 4 is the latest version of VMware's virtualization product for the Mac, and boasts a long list of new features. Fusion 4 includes an enhanced migration assistant for Windows users to facilitate that switching process. The product also includes improved support for OS X Lion, and can now run OS X Lion in a virtual machine (VM), which gives Mac power users and administrator more flexibility when running Mac OS variants in VMs.

Whereas Fusion has historically targeted the Mac consumer market, VMware Workstation has enjoyed most of its sales success in the enterprise. VMware Workstation 8 features more than four dozen new features, most designed to make it easier for administrators to work with VMs and the cloud. A new upload to vSphere option allows admins to easily copy VMs from Workstation to vSphere, and a new VM sharing feature lets users provide access to specific VMs when a multiple users need to access the same environment. Like Fusion 4, Workstation 8 also features an enhanced user interface and enhanced 3D graphics performance.

For more information about VMware Fusion and VMware Workstation 8, you can visit the new Fusion 4 (www.vmware.com/products/fusion/overview.html) and Workstation 8 (www.vmware.com/products/workstation/overview.html) product pages.

TITUS Launches Email Classification Solution

TITUS released the latest version of TITUS Message Classification (TMC), an email classification solution that provides key enhancements designed to help organizations enforce classification policy, raise security awareness, and ensure protection of sensitive data. TMC lets users quickly and easily classify, visually label, and protect emails. The latest version of TMC further integrates classification with policy enforcement capabilities. For more information, go to www.titus.com.

Drobo B1200i Delivers Automated, Application-Driven, Affordable Storage to the SMB

Drobo introduced the Drobo B1200i, a new business solution targeting the small to midsized business (SMB) market. The new 12-bay Drobo offers a storage solution for Microsoft Exchange Server, VMware, and other business applications, taking an application-driven approach to storage, cutting cost and complexity while automating modern data protection, capacity planning, and application performance. The Drobo B1200i's automated BeyondRAID technology optimizes advanced data protection without the

need for specific storage expertise or configuration. It also adjusts in real-time to changes in application workload, without the need for user or admin intervention and tuning, and it utilizes SSD technology in the same pool as conventional disk drives to accelerate the most demanding operations. The Drobo B1200i starts under $10,000 for 12TB of SAS storage. For more information, go to info.drobo.com/resources/b1200i.

Perimeter E-Security Dials In to Microsoft Office 365

Perimeter E-Security launched its Compliance and Continuity Suite for Microsoft Office 365 with enhanced continuity and e-discovery capabilities for securely capturing and storing all incoming and outgoing messages. Organizations can now archive every message, preserve uptime, and increase the accuracy of internal and external compliance reviews. Key features include message mirroring and tamper-proof storage. For more information, visit www.perimeterusa.com.

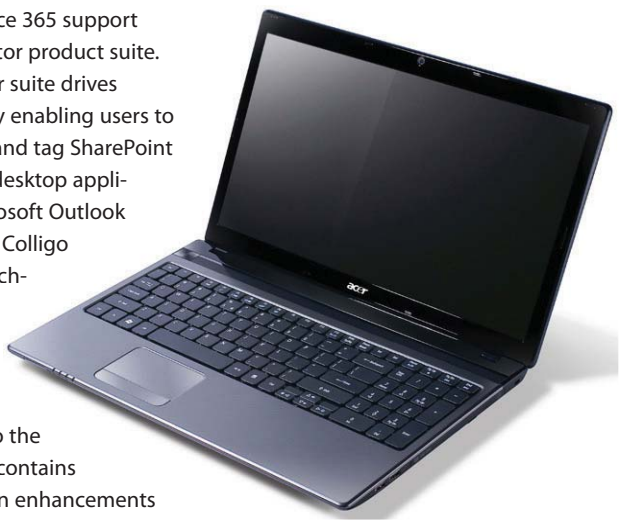
Colligo's Microsoft Office 365 Support

Colligo Networks announced that it has released Microsoft Office 365 support for its Colligo Contributor product suite. The Colligo Contributor suite drives SharePoint adoption by enabling users to easily access, capture, and tag SharePoint content from popular desktop applications, including Microsoft Outlook and Windows Explorer. Colligo Contributor's offline caching capability enables users to create, view, and edit SharePoint Online content, even when not connected to the cloud. Version 4.3 also contains several customer-driven enhancements and improvements. For more information, go to www.colligo.com.

Acer Aspire S3 Combines Best of Tablet PC and Smartphone

Traditional notebooks, tablet PCs, and smartphones each have their unique advantages in design: Notebooks provide computing power and enhance productivity, whereas smartphones and tablet PCs start up and access the Internet quickly, are small, light and easy to carry, as well as simple to operate. Acer has introduced a new generation of notebooks to satisfy these needs: the Aspire S3.

This notebook blends full PC capabilities with the advantages of tablet PCs and smartphones. Also, the ultra-thin and light design of the Aspire S3 meets the needs of modern notebook users. The open cell design of the 13.3" HD LED display contributes to the thinness and durability of the cover by using the lid and bezel to form an aluminum frame for the screen, and in the process, conserves materials. Furthermore, the high-efficiency battery requires less charging, making the Aspire S3 a greener choice for environmentally conscious buyers. For more information, visit www.acer.com



Paul's Picks

www.winsupersite.com

SUMMARIES of in-depth product reviews on Paul Thurrott's SuperSite for Windows

Windows 8 Developer Preview

PROS: Major innovations in user experience and the underlying platform; a solid foundation for client computing

CONS: Mainly a consumer-oriented release with few major advances for the enterprise; switching between new shell and old desktop is jarring

RATING: ◆◆◆◆◇

RECOMMENDATION: The new Windows 8 shell, the Start screen, not only is beautiful and usable, it augurs a new age of truly personal computing with a UI that works with touch, mouse and keyboard, or pen, and across devices with screens as small as seven inches or multiple 30-inch displays. Microsoft is using the UI for Windows Server and Xbox 360, and my sources say that Windows Phone will switch over in late 2012. Did Microsoft just yank victory from the jaws of defeat? I think so.

DISCUSSION: "Windows 8 Developer Preview" www.winsupersite.com/article/windows8/windows-8-developer-preview-140546

Windows Small Business Server 2011 Essentials

PROS: A rejiggered SBS; nice separation of cloud- and on-premises computing resources; simple AD infrastructure

CONS: Incomplete without O365 add-in

RATING: ◆◆◆◇◇

RECOMMENDATION: Windows Small Business Server 2011 Essentials is the SBS product I asked for years ago. With the same solid underpinnings as Windows Home Server 2011, it offers simple setup and management for Active Directory domains, plus centralized PC and server backup and network health monitoring, content storage and sharing, and great remote access tools. However, Office 365 and cloud-based email, contacts, calendar, and document management are not to be seen. Microsoft says they'll ship in late 2011. Then SBS 2011 Essentials will be a no-brainer.

DISCUSSION: "Windows Small Business Server 2011 Essentials" www.winsupersite.com/article/windows-server/windows-small-business-server-2011-essentials-140451

InstantDoc ID 140630

REVIEW

ExtremeZ-IP

Like many businesses, the computer environment where I work is mostly Windows-based; however, as more users opt for Macs at home, their desire to use a Mac at work seems to be trending up. There will come a time for many IT pros when it might be easier to just give the executive/marketing (etc.) department what it wants, as long as the environment doesn't become unmanageable. ExtremeZ-IP goes a long way toward filling those management gaps.

For a production environment, ExtremeZ-IP is supported on Windows Server 2008, Windows Server 2003, Windows Storage Server, or a Windows-based network access server (NAS). You can also install ExtremeZ-IP on Windows 7, Windows Vista, Windows XP Pro, or Windows XP Embedded—but this is only recommended for test environments. The minimum hardware recommendations are a Pentium 6 processor and 1GB of RAM.

I installed ExtremeZ-IP's 21-day trial software, which added the service *ExtremeZ-IP File and Print for Macintosh,* as well as two Apple Filing Protocol (AFP) volumes. (ExtremeZ-IP refers to its AFP shared folders as volumes.) The last step to get my server going was to install Windows Search on the server and add the new folder to the Windows Search indexing list. (ExtremeZ-IP uses the Windows Search indexes for its integration with the Spotlight search tool in OS X.)

Installing the ExtremeZ-IP application on the server couldn't be easier; you just run the download and click Next until it finishes. You might want to bind the Mac to Active Directory (AD) through the Directory Utility, located on the Mac under \Applications\Utilities. This way, your users will be able to log on with the same AD credentials that they use everywhere else, and you won't have to manage a bunch of local accounts.

With ExtremeZ-IP comes an application to simplify access to shared volumes and printers. The application is called Zidget, and you can install it from http://<server IP address>:8081. Zidget must be installed per user or deployed with some type of network deployment tool. After it's installed by an administrator, any user can run the installation and will be given the option to add Zidget to his or her dashboard. Zidget gives users an easily accessible list of printers and ExtremeZ-IP volumes from the Mac dashboard. From the server, I was able to specify the PPD file (Mac printer driver) and create a shared printer using the ExtremeZ-IP application. Back at the Mac dashboard, from Zidget, I expanded the location where I knew the printer was located and double-clicked the printer to install. My test print job came out without any issues.

It was practically self-explanatory to create an AFP-shared volume from the ExtremeZ-IP administrative console. Likewise, I had no problem accessing the volume from Zidget or using the *Connect to Server* feature from the OS X Finder application by entering afp://192.168.1.222/ExtremeZ-IP-Share. (My server's IP address is 192.168.1.222, and the folder I was sharing was named ExtremeZ-IP-Share.) From this volume, I copied a single file of 526MB to the Mac in about 52 seconds. After remapping the same volume with SMB (i.e., smb://192.168.1.222/ExtremeZ-IP-Share), I copied the same 526MB file from the server to the Mac but this time in about 65 seconds. I tried a similar test with a folder containing about 7.6GB of images; again, the ExtremeZ-IP (AFP) source was faster: 33 minutes versus 38 minutes for the SMB share. One thing to keep in mind is that just because you use ExtremeZ-IP to create a volume doesn't mean you automatically have a corresponding SMB share. ExtremeZ-IP uses AFP to share folders—so if you want your Windows users to access the same share as your Mac users, you need to share the same folder again, but using the standard Windows sharing steps. Unless your Windows client computers are running AFP as a networking protocol, they won't be able to see or access the ExtremeZ-IP volumes.

In addition to performance improvements around file sharing, I tested the volume restriction capabilities of ExtremeZ-IP. In the volume settings, there are two attributes for controlling access: *Volume is read-only* and *Allow guests to use this volume.* You can also assign a password to the volume and limit the number of users. However, as with Windows SMB shares, the NTFS permissions are in effect and the most restrictive settings will apply. ExtremeZ-IP volumes must be on a drive formatted with NTFS.

A common problem with Mac/Windows integration in the past has been the way Macs have used *resource forks* to optimize the performance of documents containing objects such as images or just to store certain file attributes. The resource fork information is typically stored in a dot-underscore file and hidden to Mac users. Windows users can see these files and have been known to delete them for no particular reason. Of course, this creates a big mess for everyone. After multiple edits with Microsoft Word for Mac 2011, and searching the server, I didn't see any dot-underscore files in the ExtremeZ-IP volume I was accessing the document from—although the ExtremeZ-IP application on the server indicated that there were multiple resource forks. I tried the same thing with OpenOffice 3, and this time I could see that a resource fork file existed in the folder where the actual document was located when I viewed the directory from Windows. After I saved my changes, the resource fork was gone and the dot-underscore file disappeared.

Another common problem facing administrators of Mac/Windows integrated environments, especially when older versions of Windows are in use, is the incompatibility of naming options on the Mac versus the file naming option within Windows. For example, on a Mac, the slash character (i.e., /) can be used in a filename. ExtremeZ-IP gives administrators the ability to prevent Mac users from saving files with these characters or with exceptionally long filenames that might also cause problems with their Windows users, by disallowing the use of such characters or specific filename lengths in the volume filenames. Enabling this feature is as simple as checking a box and adjusting the ExtremeZ-IP application's Filename Policy options, as Figure 1 shows. There's an option to apply the file naming policy to all volumes; alternatively, you can go to the

Nate McAlmond | mcalmond@gmail.com

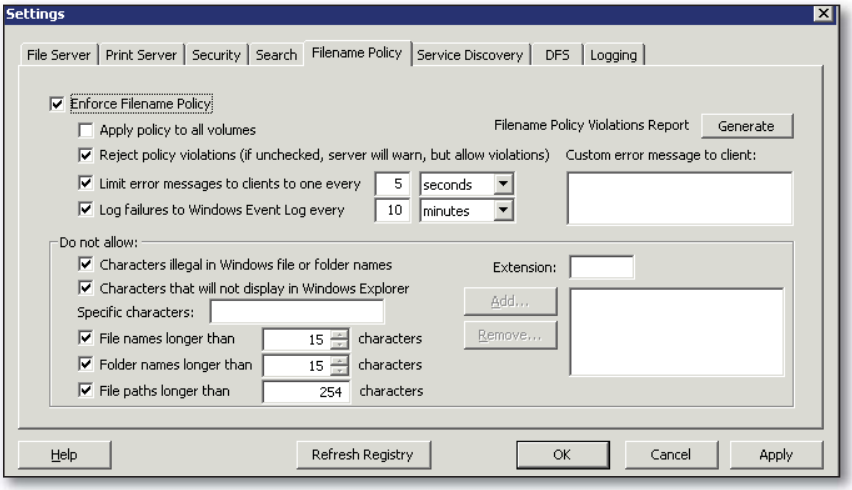


Figure 1: Applying filename restrictions in ExtremeZ-IP

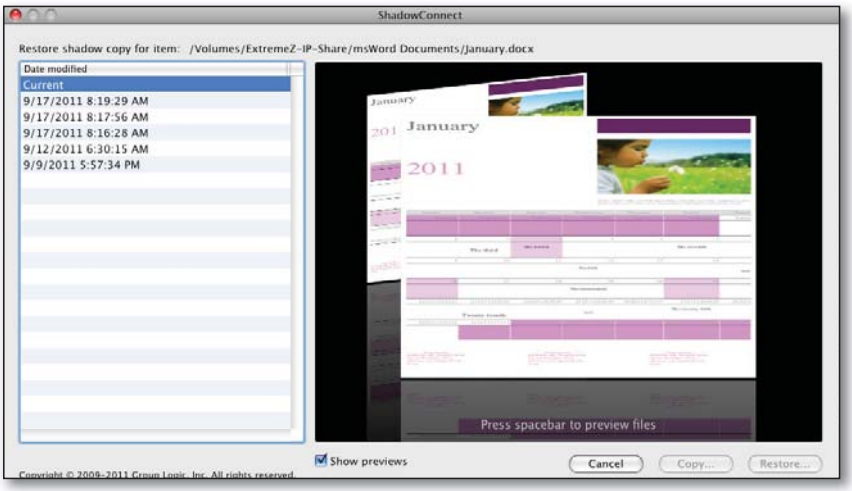


Figure 2: Using ExtremeZ-IP's ShadowConnect software to restore files

specific volume's settings and enable the file naming policy there. After applying the default file naming policy and choosing the global option to apply the policy to all the volumes, I tested the settings back at the Mac and found that they had taken effect immediately.

One of the options when creating a share with ExtremeZ-IP is the ability to make the share compatible with the Mac's backup system, called Timemachine. To turn this feature on, go into the particular volume's settings, select the *Support Timemachine backup* check box, and click OK. To test this feature, I turned on Timemachine support for one of the ExtremeZ-IP volumes and started a backup using Timemachine from the Mac. After a few hours, the Mac's 100GB backup completed successfully. You'll probably want to limit this feature to non–file sharing volumes, because turning on support for Timemachine also turns off search support.

With Windows Search (a free Microsoft download) installed on the ExtremeZ-IP server, the Mac's built-in Spotlight search tool can be used to search ExtremeZ-IP volumes. Just be sure to add the volume to the Windows Search indexing list on the ExtremeZ-IP server and search under Shares within Spotlight. When I tried this feature, Spotlight searched the Mac's hard drive and didn't give me the results I expected. But as soon as I selected the volume I meant to search, I received the expected results.

Another ExtremeZ-IP feature I tested was its version tracking/recovery of documents. Configuring Microsoft Volume Shadow Copy Service (VSS) copies on the server and installing ExtremeZ-IP's ShadowConnect client software (downloaded from the server at http://<server IP address>:8081) lets Mac clients right-click files from an ExtremeZ-IP volume and choose to restore from previous versions. When restoring, you can choose an alternative location and not overwrite the existing version. You even get a preview screen of each version, as Figure 2 shows, so you can decide if it looks like the correct document before you restore it. After some experimentation, I could tell that ExtremeZ-IP does its version tracking by comparing the VSS copies on the server—so the number of versions available to your end users will depend on how frequently you configure shadow copies to be created on the server and how often end users save their changes.

The one area where I had problems relates to using ExtremeZ-IP with a DFS share that I was trying to automatically mount on login. I wasn't able to consistently get the product to access a DFS link where the domain name was used in the name space (e.g., //example.com/dfs-root). I had no problems mapping to a server and folder within the DFS (e.g., afp://server.example.com/dfs-root). Also, at press time, DFS integration wasn't supported on Apple's most recent OS version, code-named Lion. I contacted an ExtremeZ-IP representative and learned that there are known issues with OS X 10.5 and that my problem was most likely that OS X wasn't unmounting correctly upon logging off. According to the representative, my problem would probably be resolved if I upgraded to OS X 10.6.

ExtremeZ-IP brings a lot to the table. The number of features the tool provides greatly simplifies the administrator's job of integrating Macs into a Windows server environment. In addition, tools such as Zidget and the performance gains of using AFP should go a long way toward making end users happy and more productive.

InstantDoc ID 140693

ExtremeZ-IP

PROS: Quick; easy to set up and manage; improves network performance and end-user experience

CONS: Problematic integration with DFS

RATING: ◆◆◆◆◆

PRICE: $1,995 for a 25-client server; $4,495 for a 100-client server

RECOMMENDATION: Anyone who needs to integrate Mac OS X clients with a Windows server environment should consider using ExtremeZ-IP.

CONTACT: GroupLogic • 703-528-1555 • www.grouplogic.com

REVIEW

Social Sites for SharePoint 2010

More and more organizations are embracing social media not just to communicate with customers and partners, but between employees as well. Rather than using external sites, such as Facebook or LinkedIn, where sensitive information might accidentally be made public, dedicated solutions are increasingly seen as desirable. These dedicated social media sites for employees can be hosted internally or externally and can either be standalone or integrated into other technologies such as corporate email, instant messaging, and collaboration suites.

Enter Social Sites for SharePoint 2010 from NewsGator Technologies. Social Sites extends an existing Microsoft Office SharePoint Server 2010 deployment to add a host of collaborative social media functions, such as blogging, communities, ad hoc question and answer capabilities, news feeds, video streaming, and more.

To get started with Social Sites, you need an existing installation of SharePoint 2010. Your installation must be an enterprise deployment: that is, you must have Active Directory (AD), with SharePoint configured to use AD as the identity store. I also discovered that you must have a configured and working My Site, even if you choose not to deploy to it. Installation isn't for the faint of heart if you don't have a vanilla SharePoint installation, or if your AD and networking configuration aren't standard. The installation guide, although densely written, does walk you through these issues and gives pointers to solutions. After you address these problems (if necessary), installation becomes relatively easy.

Before launching the setup, you must configure a SharePoint administrator account with the necessary permissions to your SharePoint farm and services. I had to run the setup from my SharePoint server's hard drive in a writeable folder so that the setup could write out the installation log and a configuration file for later use in unattended installations. One disconcerting problem I had was that I could only start setup if I configured the administrator account for the domain as the SharePoint administrator account and ran setup from that. Depending on the options you're installing, you need to configure an account that email notifications are sent from, as well as various Web Application Pools and their identities—but these are common requirements for many SharePoint applications.

Be sure to schedule installation during a maintenance window; during installation, my SharePoint farm became unavailable at times as various services were stopped and configured. I also experienced a problem in which I didn't deploy Social Sites to a web application that I wanted to, because of a mistake on my part. I had to completely uninstall Social Sites and reinstall it, rather than adding it to the site I wanted using the Repair option, as documented in the installation guide.

If you perform a standard installation and deploy Social Sites to your My Sites, your users will immediately see that the standard My Sites web parts and page have been replaced with the Social Sites web parts. On the left-hand side of the page is the Activity Stream, where users can post details of what they're doing, make a general comment or observation, ask a question, or post a private message to another user. Users can flag postings that they like, add comments, share them, or mark them for follow-up. Answers to questions can be marked as the correct answer. Social Sites allows users to add personal subscriptions in the form of RSS feeds and tweets from Twitter. Users can register topics of interest to them and will receive tailored notifications or email messages containing those items or digests of items, depending on how they choose to receive the information. The Activity Stream refreshes itself, so users see updates as they occur. Each user can configure a comprehensive range of profile information and settings, including the ability to register activities he or she wants to follow, such as people receiving badges for activity, people changing job titles or managers, and profile updates.

The right-hand side of the page contains Communities, which need to be configured before they can be used. Communities are created as SharePoint websites, using templates that are added to your SharePoint farm. You can find these templates under the NewsGator tab in the Template Selection section of the New SharePoint Site webpage, which you access from Site Actions. Communities can be public or private; the private setting lets you restrict access. Users can join any public or private community that they have access to. Community members can send posts to all other members of the same community using the community name, and the posts appear in everyone's Activity Stream and on the community home page. Community sites can have document and picture libraries, microblogs, question lists, discussion boards, and surveys, as well as subsites and workspaces. Communities are easy to search and join.

Social Sites does an excellent job of extending SharePoint with social media functions. It's easy to get communities up and running, and employees can quickly start communicating and tracking communities, activities, and each other.

InstantDoc ID 140476

Social Sites for SharePoint 2010

PROS: Intuitive; easy to use; immediately useful

CONS: Requires a standard, enterprise SharePoint farm; domain administrator account necessary for installation; must uninstall and reinstall the product to deploy to a new web application, rather than simply extend its features

RATING: ◆◆◆◆◇

PRICE: Starts at $2 per user per month

RECOMMENDATION: You should consider Social Sites if your company wants to offer employees an in-house social media solution and you're an experienced SharePoint administrator who is comfortable managing a highly complex social media toolset.

CONTACT: NewsGator Technologies • 800-608-4597 • www.newsgator.com

John Howie | jhowie@microsoft.com

ToughTech mini-Q

Data security is always a hot topic for IT professionals, and recent headlines have underscored the need for a rigorous approach to data security. The need for a more aggressive security approach extends to removable storage devices, such as USB flash drives, hard drives, and other locally attached storage devices. WiebeTech's ToughTech mini-Q external hard drive seems well-positioned to fill that need. The ToughTech provides several security features that could make it a valuable tool in any administrator's toolbox.

My review unit was WiebeTech's ToughTech mini-Q drive with WriteLock; it came shipped with a pre-installed 500GB Serial ATA (SATA) 2.5" hard drive. WiebeTech typically sells the ToughTech as an empty enclosure without a hard drive, and customers can install their own 2.5" SATA hard drive of up to 750GB capacity. It's important to note that only 9mm or thinner drives will fit within the ToughTech enclosure, so make sure to measure the thickness of any drives you plan on installing. The ToughTech also supports installation of solid state disk (SSD) drives of acceptable size.

The ToughTech ships with a plethora of cables and connection types. I counted support for four different connectors, including FireWire 400 (via adapter cable), FireWire 800, external SATA (eSATA), and USB 2.0. I was a bit disappointed to see that support for USB 3.0 or Thunderbolt wasn't included, but WeibeTech might consider supporting those connection types in future versions of the ToughTech. The product also ships with connection cables for all the ports I mentioned, as well as an AC adapter, a small screwdriver (for installing your own drive), three hardware AES-128 encryption keys, and three lanyards for those keys. That's an impressive number of supporting accessories for a single product, and they all help make the ToughTech a more useful storage device for a wide array of use cases.

After I unpacked the drive and all the related cables, installing the ToughTech was as simple as plugging in the AC adapter and connecting the drive to my laptop via USB cable. An OEM copy of Prosoft Engineering's Data Backup PC 3 is included for helping with file backup duties. The ToughTech is compatible with most modern OSs with USB 2.0 support, including Windows 7, Windows Vista, and Windows XP; Mac OS X; and many Linux distributions. For this review, my primary test computer was a Dell Latitude D630 laptop using a USB 2.0 connection running Windows 7 Enterprise.

The particular model of the ToughTech that I tested requires the use of an AES-128 (FIPS-197 listed, certification number 60) hardware-based encryption key to operate, which takes the form of a small chunk of black rubber that includes a mini USB connector on one end and a hole for the lanyard on the other. In order for the drive to operate, the key has to be inserted into a mini-USB connector on the front faceplate of the drive. Remove the key, and any data you have on the drive will be inaccessible until the key is reinserted.

The ToughTech ships in a textured aluminum enclosure, which serves double-duty as a heat sink—drawing heat away from the drive—and giving the drive a bit more protection from physical impacts and jolts than a traditional USB hard drive might have. The aluminum casing doesn't extend to the front and rear panels, which are both silver-colored plastic. The ToughTech also ships with shock-dampening strips between the bottom of the drive case and the aluminum shell, which gives the drive additional protection against jolts, shocks, and bumps. The ToughTech did slip off a low table during testing and has operated without any problems since then.

I used the ToughTech for several weeks, copying files back and forth from a variety of PCs to the drive. I also tried to access the drive without the key installed. It definitely works as advertised; the files were inaccessible without the AES key inserted into the drive. Drive performance can vary widely depending on what 2.5" drive you choose for the enclosure, but in my testing the drive copied files and data just as quickly as some other, non-secure USB hard drives I've looked at.

If you're looking for an external USB hard drive solution that offers more storage and security than traditional USB flash drives, you can't go wrong with the ToughTech. An all-aluminum case design and USB 3.0 support would have bumped my review up by at least a half a star, but as-is the ToughTech is a fine choice for security-minded admins looking for additional portable storage.

InstantDoc ID 140533

ToughTech mini-Q

PROS: Quick and easy installation; straightforward AES-128 key concept; clear and comprehensive instructions; numerous cables, adapters, and other accessories included

CONS: Can be pricey; some plastic case components; no USB 3.0 or Thunderbolt support

RATING: ◆◆◆◆◇

PRICE: $499.99

RECOMMENDATION: It's not perfect, and it can get expensive—but the ToughTech mini-Q is a fine choice if you're looking for an external hard drive solution for sensitive files and documents that's more secure than other removable backup options.

CONTACT: WiebeTech • 866-744-8722 • www.wiebetech.com

Jeff James | jjames@windowsitpro.com

Enterprise SSDs

Streamline your storage with flash technology

by Jason Bovberg

It's easy to see why SSDs are experiencing a storm of activity in the storage realm. They're fast! Traditional disks obviously have to rotate, taking a *whopping* 5 milliseconds to get to your data. SSDs are fundamentally different, offering microsecond lookup times. Because of this simple latency difference, SSDs give you an instantaneous way to boost system and application performance. The metaphor that Texas Memory Systems' Jamon Bowen likes to use is the CPU. "Let's say you have a CPU-bound app, and you drop in a CPU that's five times more powerful. That app runs five times faster. SSD offers essentially the same paradigm."

Traditionally, the downside of SSDs has been cost; often, the added performance just hasn't been worth it. "But SSDs offer so much capacity now!" says Bowen. There are a multitude of enterprise SSD offerings on the market, and this Buyer's Guide covers a few of your options for the sake of quick comparison. But before you dive into the market, you need to know about some key differentiators that are important to your buying decision.

SLC vs. MLC

To focus this buyer's guide, I established a general distinction between consumer and enterprise SSDs. The best way to make such a distinction is to look at single-level cell (SLC) versus multi-level cell (MLC) chips. If we're talking about an enterprise application, the trend is toward SLC—and that's where a lot of the cost differential comes from. MLC is half the price automatically because of its ability to store two bits per cell, but you have less margin for error when reading data, so it's more error-prone. The main concern people have about flash in general is its ability to hold up over time under heavy write workload. And in that kind of environment, SLC wins. Yes, it's twice as expensive, but it also lasts more than twice as long.

Key Considerations

While shopping for your SSD solution, keep three particular considerations in mind (beyond each vendor's performance claims, such as the amount of time under particular write workload that the drive is rated to last): Mean Time Between Failures (MTBF), TRIM compatibility, and wear leveling.

MTBF. One thing that separates enterprise and consumer drives is their ability to handle failures internally. "Just because a flash chip has no moving parts doesn't mean that failures won't occur," says Bowen. "They will." MTBF is about how much redundancy has been built into a device to handle those failures.

TRIM compatibility. SSDs don't write data randomly; they store data in blocks that are moved around by a flash translation layer (FTL) as you update it. Over time, data is rewritten, and some data ends up in the background that isn't referenced by anything anymore. That data needs to be deleted so you can write to the space again. The TRIM standard allows for the OS to inform the SSD that it has deleted a file.

Wear leveling. Media wears out. SSDs' blocks can go through only so many erase cycles before they begin to become unreliable. Wear leveling arranges data so that erasures and re-writes are distributed evenly, so that the SSD doesn't wear out unevenly.

SSDs in the Enterprise

A core distinction between enterprise and consumer SSDs is the power of the controller in front of the flash memory, and how it handles SSDs' inherent random-write disadvantages. "That's what's most difficult for a flash controller, and where virtually all performance R&D goes," says Bowen. The problem in the SSD market is that although the controller is the most important SSD component, it hasn't been standardized so that you can easily say one SSD is better than another without running random-write workload tests. So you have some research and work ahead of you. But this buyer's guide is at least a good starting point.

InstantDoc ID 140604

JASON BOVBERG
(jbovberg@windowsitpro.com) is a senior editor for *Windows IT Pro* and *SQL Server Magazine*, covering products as well as the systems management, hardware, and storage/backup topic areas. He has 25 years of experience as a writer and editor in magazine, book, and special-interest publishing.

What About Hybrid?

The goal of hybrid SSD solutions is to lower cost and make storage more effective. "Legacy storage solutions are pretty hard to use and require lots of specialized training and lots of understanding about how storage internals work," says Keith Hageman, storage technology evangelist at XIO (whose Hyper ISE won big at this year's Microsoft TechEd conference). "Hard drives have gone from megabytes to terabytes. By combining hard disks and SSDs, we can tackle the capacity performance problems that hard disks don't solve. As a result, the customer should see a drastic reduction in footprint." The big benefit of a hybrid solution is that it tackles the storage problem from an infrastructure perspective: You add the SSDs, and it makes storage more effective. You can use bigger drives plus SSDs to get better performance. But to be truly effective, it has to be unified with all your other storage.

Company	Product/Series	Pricing	Weight	Capacity	SLC or MLC	Power Consumption
BiTMICRO Networks 510-623-2341 www.bitmicro.com	E-Disk Altima	Contact vendor	3 oz. to 9.1 oz. (2.5"); 9.6 oz. to 29.4 oz. (3.5")	1.1TB	SLC	Contact vendor
	E-Disk Altima	Contact vendor	3 oz. to 9.1 oz. (2.5"); 9.6 oz. to 29.4 oz. (3.5")	1.1TB	SLC	Contact vendor
Dataram 609-799-0071 800-328-2726 www.dataram.com	XcelaSAN	Starts at $65,000	65 lbs.	128GB or 256GB FC SAN cache	N/A	600W
Fusion-io 801-424-5500 www.fusionio.com	ioDrive Duo 1.28TB	Contact vendor	Contact vendor	1.28TB	MLC	Contact vendor
	ioDrive Duo 640 GB	Contact vendor	Contact vendor	Contact vendor	SLC	Contact vendor
	ioDrive 320GB	Contact vendor	Contact vendor	320GB	SLC	Contact vendor
	ioDrive	Contact vendor	Contact vendor	160GB	SLC	Contact vendor
	ioDrive Octal Capacity	Contact vendor	Contact vendor	5.12TB	MLC	150W
Gridiron Systems 408-470-4500 www.gridironsystems.com	TurboCharger GT-1100	$140,000	54 lbs.	Up to 6.5TB	eMLC	430W
Micron Technology 208-368-4000 www.micron.com	Real SSD P320h	Contact distributor	5.1 oz. (350GB), 5.4 oz. (700GB)	350GB, 700GB	SLC	Active 25W, idle 6.1mW
	Real SSD P320h	Contact distributor	5.1 oz. (350GB), 5.4 oz. (700GB)	350GB, 700GB	SLC	Active 25W, idle 6.1mW
	Real SSD P300	Contact distributor	Less than 3.5 oz.	50GB, 100GB, 200GB	SLC	Idle 125mW, active varies by capacity
Nimbus Data Systems 415-651-4646 877-664-6287 www.nimbusdata.com	Nimbus S-class Sustainable Storage Platform	Starts at $24,995	72 lbs.	2.5TB to 10TB	eMLC	300W per system
OCZ Technology 408-733-8400 800-459-1816 www.ocztechnology.com	Z-Drive R4	Contact vendor	4.59 oz.	300GB–2TB	SLC and MLC	Active 12.3W, idle 9.3W
	Deneva 2	Contact vendor	3.1 oz.	60GB–480GB	MLC	Active 2.7W, idle 1.5W
STEC 949-476-1180 800-367-7330 www.stec-inc.com	MACH16 SSD	Contact vendor	Less than 3 oz.	400GB	SLC and MLC	7.5W
	Kronos PCIe SSA	Contact vendor	Contact vendor	1.95TB	SLC and MLC	25W
	ZeusIOPS SSD (gen 4)	Contact vendor	Less than 15 oz.	1.6TB	SLC and MLC	9W
Texas Memory Systems 713-266-3200 www.ramsan.com	RamSan-440	$80,000–$140,000	90 lbs.	128GB to 512GB	DDR RAM	650W
	RamSan-630	$51,850–$314,500	55 lbs.	1TB to 10TB	SLC	500W
	RamSan-710	$45,000–$150,000	25 lbs.	1TB to 5TB (usable)	SLC	280W
	RamSan-70	$14,500–$28,000	Contact vendor	Contact vendor	SLC	25W, 40W
Violin Memory 650-396-1500 www.violin-memory.com	Violin 3100 series flash memory arrays	Starts at $325,000	75 lbs.	40TB	MLC	800W
	Violin 3200 series flash memory arrays	Starts at $150,000 (5TB)	70 lbs.	20TB	SLC	500W
XIO Storage 719-388-5550 866-472-6764 www.xiostorage.com	XIO Hyper ISE 14.4H	Contact vendor	120 lbs.	14.4TB pre-RAID	Enterprise MLC coupled with HDD in the same pool (SHD)	600W

	Interface	Rated Read/Write Performance	Rated IOPS Performance	MTBF	TRIM Compatibility (Y/N)	Wear Leveling	Warranty
	SATA, PATA, SCSI Narrow, Ultra320 SCSI, Fibre Channel	Contact vendor	Contact vendor	1.1 million hours	No	Contact vendor	Contact vendor
	SATA, PATA, SCSI Narrow, Ultra320 SCSI, Fibre Channel	Contact vendor	Contact vendor	1.1 million hours	No	Contact vendor	Contact vendor
	Fibre Channel, zoned into Fabric	450,000 read/450,000 write	450,000 IOPS	Contact vendor	Contact vendor	Contact vendor	1 year
	PCI-Express x4/x8 or PCI-Express 2.0 x4	150,000MBps	278,000 IOPS	Contact vendor	Yes	Dynamic	5 years
	PCI-Express x4/x8 or PCI-express 2.0 x4	236,000MBps	252,000 IOPS	Contact vendor	Yes	Dynamic	5 years
	PCI Express x4	119,000MBps	135,000 IOPS	Contact vendor	Yes	Dynamic	5 years
	PCI-Express x4	123,000MBps	140,000 IOPS	Contact vendor	Yes	Dynamic	5 years
	PCI-Express 2.0 x16	72,900MBps	1,190,000 IOPS	Contact vendor	Yes	Dynamic	5 years
	Fibre Channel	Contact vendor	350,000 IOPS	45,000 hours	Yes	Dynamic	1 year
	PCI Express	Up to 3/2GBps(2)	Up to 750,000/200,000 IOPS(3)	2 million device hours	N/A	Yes (static and dynamic)	3 years
	PCI Express	Up to 3/2GBps(2)	Up to 750,000/200,000 IOPS(3)	2 million device hours	N/A	Yes (static and dynamic)	3 years
	SATA	Up to 360/275MBps	Up to 60,000/45,000 IOPS	2 million device hours	Yes	Yes (static and dynamic)	3 years
	Networked: FC, 10GbE, Infiniband	8,000MBps	800,000 IOPS	2 million hours	Yes	Dynamic	5 years
	PCI-Express 2.0 x8	Up to 2900/2700MBps	400,000 (4K Random Write)	2.5 million hours	Yes	Dynamic	3 years
	SATA 6Gb/s	525/500MBps	60,000 IOPS (4K Random Write) Up to 85,000 IOPS	2 million hours	Yes	Dynamic	3 years
	SATA	Up to 250MBps sustained reads and up to 180MBps sustained writes	Up to 26,000 random read IOPS and up to 16,000 random write IOPS	2 million hours	N/A	Yes (static and dynamic)	5 years limited (SLC) and 3 years limited (MLC)
	PCI Express	Up to 2GBps sustained reads and up to 2GBps sustained writes	Up to 220,000 random read IOPS and up to 200,000 random write IOPS	2 million hours	N/A	Yes (static and dynamic)	5 years limited
	SAS and Fibre Channel	Up to 500MBps sustained reads and up to 360MBps sustained writes	Up to 120,000 random read IOPS and up to 70,000 random write IOPS	2 million hours	Yes	Yes (static and dynamic)	5 years
	4 Gbps Fibre Channel	4.5GBps	600,000 IOPS	N/A	No	N/A	1 year
	8 Gbps Fibre Channel or QDR InfiniBand	10GBps	1,000,000 IOPS	N/A	No	Dynamic	1 year
	8 Gbps FC / QDR InfiniBand	5GBps	400,000 IOPS	N/A	No	Dynamic	1 year
	PCIe	2GBps	600,000 IOPS	1 million hours	No	Dynamic	1 year
	Direct Attach: PCIe (x4, x8); Network Attach: 4/8 Gb FC, 10 GbE	1200MBps read/ 500MBps write	Upt to 300,000 IOPS	2.1 years (system)	Yes	Dynamic	5 years
	Direct attach PCIe (x4, x8); Network attach 4/8Gb FC, 10GbE	1400MBps read/800MBps write	Up to 340,000 IOPS	2.1 years	Yes	Dynamic	5 years
	Fibre Channel	1.2GBps read/600MBps write	200,000 IOPS	1.5–3 million hours	No	Static	5 years, free standard hardware warranty

INSIGHTS FROM THE INDUSTRY

Yale Student Info Accessible via Google Search

We're normally flooded with news about hackers who bypass security systems and exploit zero-day vulnerabilities to gain access to sensitive systems—but recent news from Yale University underscores that the vast majority of IT security failures are caused by human error, neglect, or plain ignorance. According to Yale's student newspaper, the University notified 43,000 staff, students, and alumni that sensitive personal information (e.g., names and Social Security numbers) was inadvertently made accessible to Internet searches when a file was left unprotected and unsecured on an FTP server that was used as a storage location for open-source software. Zoe Gorman at the *Yale Daily News* interviewed Yale Information Technology Services (ITS) director Len Peters, who pointed to a 2010 change in Google search that allowed the search engine to locate and index content on FTP servers. Peters said that Yale ITS wasn't aware that Google made the change, which resulted in the file being accessible through Google search.

Yale University spokesman Tom Conroy released a statement about the incident, which describes measures the university will take to rectify the data breach and help prevent the individuals affected from being victims of identify theft and other security-related ills. "Yale has established a Response Center for affected individuals and is offering free credit monitoring, identity theft insurance, and other assistance to all of the affected persons," Conroy said. "A data security firm will monitor credit files at all three major United States credit bureaus for 24 months and alert individuals if a new United States credit account is opened using their Social Security number. The University takes seriously the obligation to protect personal data that is entrusted to it, and regrets the error that made the computer file accessible."

—Jeff James

InstantDoc ID 140325

Exchange Server 2010 Deployment Trends

Microsoft Exchange Server expert Michael B. Smith has a technology career spanning almost 30 years. His first IT job was in college, in the early 1980s. After working for a few different companies over the years in IT departments, in 1999 he started working in IT consulting, working largely with building hosted Exchange environments. He started his own consulting company in 2007. Michael published his first article in 1984 in *Byte* magazine, and since then he's written a couple hundred articles, over 400 blogs, 2 books, and contributed to 4 other books. Let's see what Michael has to say about the current state of Exchange server deployments.

BKW: Exchange 2010 has been available for about 2 years. What do you see as the major trends related to implementing this version?

MBS: Deployment of Exchange 2010 actually continues to accelerate at this time. I believe this is tied primarily to hardware refresh cycles and the fact that Exchange 2003 was "good enough." While Exchange 2007 and Exchange 2010 have a number of great features, for the average company, Exchange 2003 was "good enough." Because of that, many companies are interested in knowing how best to move forward with Exchange. Today, there are more options than ever. With Exchange virtualized, or in the cloud, or on premises—Exchange continues to provide great value and a great feature set for almost every company.

BKW: What situations or what type of organizations are best suited to making the move to the cloud?

MBS: I think the best match is from companies who really use Exchange only for basic email. They don't treat Exchange as a differentiator that helps provide extra value to their company. Those people can most easily move their message and communication infrastructures to the cloud. Companies that designed and built applications and operational infrastructures around the feature content of Exchange will have a greater deal of difficulty in making the move.

BKW: Considering the recent, well-publicized outage of Office 365, how should customers prepare for such outages if they do make the move?

MBS: There's no such thing as perfect uptime. Four nines (99.99%) is very difficult to attain. When planning for infrastructures to support highly available and fault-tolerant services, people come into play. And people make mistakes. That's going to be true at whatever provider you use. Based on what I've heard, this most recent issue was caused by a relatively minor design flaw that didn't provide redundant hardware services at a particular point in the switching/routing matrix—and that problem has now been corrected.

Does that make up for 3 hours of downtime? Does the financial refund of 25 percent of a month's fee make up for that? No. In US dollars for the basic service, that's only $1.50 per user. If a company needs complete control and complete accountability—then they need to continue to run their on-premises Exchange server.

I see the major issue, long-term, being Internet service. While large cities in the United States have reliable, inexpensive, high-speed Internet, that isn't true in much of the country. For example, while visiting Seattle 2 weeks ago, I noticed advertisements for $19.95 per month for 12Mbps DSL. Guaranteed for 5 years! In my hometown, $19.95 per month buys you 512Kbps DSL—25 times slower—from the same national provider, CenturyLink. And I don't buy the cheapest service, but I've had five DSL outages this year. That would be devastating to a larger company—and is certainly painful for me! Since you can't access email when you can't get to the Internet, you have to calculate what that cost is to your business.

BKW: What does a business need to keep in mind to determine which is the appropriate architecture for their organization?

MBS: The number-one consideration is I/O load. While relatively minor with today's hypervisors, I/O operations taking place within a hypervisor are marginally slower than on a physical server. If you design hardware very close to its physical limits, that can be challenging. And people like to run virtual machines with too little memory—especially on VMware. Exchange is memory hungry. Don't think that you can effectively run an Exchange server in a VM and reduce its memory below recommended values and still get good performance.

—B.K. Winstead

InstantDoc ID 140407

Systems Administration Is the Art of Operationalizing Pessimism

If something can go wrong, it will go wrong. This usually happens at about 4:50 P.M. on a Friday afternoon when you've got reservations for a meal at a nice restaurant with your partner later that evening. It's even more likely if you've organized a babysitter for the evening. Nothing attracts bad luck like the possibility of extreme inconvenience.

This is when the whole idea of the cloud sounds awesome—because surely if you used the cloud you wouldn't have a storage array on the SAN in your data center try to chew itself to pieces in some sort of bizarre late Friday afternoon suicide ritual. Well, it might happen—but that's the cloud's problem and not yours. Perhaps infrastructure outsourcing is a more direct method of redirecting bad system karma to another team of geeks.

I'm not sure how superstitious most systems administrators are, but I'm definitely one who assumes that if someone says, "It can't get any worse than this," then odds are that the universe is going to find a way to prove that statement incorrect.

Systems administration is the art of operationalizing pessimism. You think of ways that stuff can go wrong and then you come up with a workaround. You back up data in case it becomes corrupted or the hosting disk fails. You use clustered servers so that if one server fails spectacularly, you've got another server there to take the load. You use redundant networks so that if one switch or router decides to fry its internal electronics, you've got another one that will quietly keep the packets flowing.

But you don't need to cluster everything, and you don't need redundant networks everywhere. In some cases you'll be fine with the downtime it takes to put together spare network hardware and replace it, rather than spending money so that each piece of network hardware has a failover. You don't need to host every SQL Server database on a failover cluster. In a lot of situations, just replicating to another SQL Server box will be adequate.

One of the problems that systems administrators face is that as human beings, we aren't very good at assessing risk. That's why we get panicky about the possibility of sharks when swimming at the beach in the summer. But we don't really worry about the drive down to the beach, even though, statistically, we're more likely to come to harm on the drive than in the water.

In some ways, a lot of profit in the IT security industry is based on the inability to assess risk. It's easier to sell a solution to a scary problem than it is to sell a solution to a more prosaic problem.

As a systems administrator, it's necessary to be rational about pessimism. Systems administrators have a limited amount of resources and time, so it's natural to protect against the things that are likely to cause problems. It isn't the one-in-a-million events that systems administrators need to deal with first (with apologies to Terry Pratchett's Discworld probabilities), but the one-in-a-thousand events and the one-in-ten-thousand events. Figuring out the precise probabilities of certain events occurring is very difficult, but when you're assessing risk, try to prioritize your risks into "more likely" and "less likely" events.

If you deal with the more likely risks first, you're also more likely to be able to make that dinner with your better half at 7:00 P.M. on Friday night instead of spending it knee-deep in the guts of a server finding creative ways to use expletives to describe your precise views about the profession of systems administration.

—Orin Thomas

InstantDoc ID 140277

Statement of Ownership

Statement of Ownership, Management, and Circulation for *Windows IT Pro Magazine* as required by 39 U.S.C. 3685; *Windows IT Pro,* publication no. 1552-3136, filed October 1, 2011, to publish twelve monthly issues each year for an annual subscription price of $49.95. The mailing address of the office of publication is 748 Whalers Way, Fort Collins, CO, 80525. Peg Miller, Publisher, and Amy Eisenberg, Editor, at the same address. The owner is Penton Media Inc., 249 W. 17th St., 4th Floor, New York, NY 10011-5390. Penton Business Media Holdings, Inc., of 249 W. 17th St., 4th Floor, New York, NY 10011-5390, owns 100% stock in Penton Media, Inc. The average number of copies of each issue published during the twelve months preceding the filing date include: total number of copies (38,531); outside county paid mail subscriptions (17,637); sales through dealers and carriers, street vendors, and counter sales and other non-USPS paid distribution (4,374); paid distribution through other classes of USPS mail (155); total paid circulation (22,166); free or nominal rate distribution by mail (11,596); free or nominal rate distribution outside the mail (2,293); total free or nominal rate distribution (13,889); total distribution (36,055); copies not distributed (2,476); for a total of (38,531) copies. The actual number of copies of single issues published nearest to the filing date include: total number of copies (34,361); outside county paid mail subscriptions (16,116); sales through dealers and carriers, street vendors, and counter sales and other non-USPS paid distribution (3,954); paid distribution through other classes of USPS mail (62); total paid circulation (20,132); free or nominal rate distribution by mail (11,455); free or nominal rate distribution outside the mail (921); total free or nominal rate distribution (12,376); total distribution (32,508); copies not distributed (1,853); for a total of (34,361) copies.

I certify that the statements made by me above are correct and complete.

—Peg Miller, Publisher

AD INDEX

For detailed information about products in this issue of *Windows IT Pro*, visit the websites listed below.

COMPANY/URL	PAGE
Altova www.altova.com	3
Centrify www.centrify.com	CD Outsert
GFI www.loveyourav.com	Cover 3
IBM Corporation www.ibm.com/facts	Cover 2,9
IBM Corporation www.ibm.com/systems/blade	25
Microsoft www.microsoft.com/office365	Cover 4
NetWrix www.netwrix.com	6
Paul Thurrott Pocket App www.windowsitpro.com/mobile-apps	18
Privacyware www.privacyware.com	61
Western Governors University www.WGU.edu/ITPro	60
WinConnections Spring 2012 Event www.WinConnections.com	Cover tip, 46
Windows IT Pro e-Learning Series http://elearning.left-brain.com	56

VENDOR DIRECTORY

The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

Acer 51	Fusion-io 58	Nimbus Data Systems 58	TITUS 50
BiTMICRO Networks 58	Google 60	OCZ Technology 58	Violin Memory 58
Colligo Networks 51	Gridiron Systems 58	Perimeter E-Security 51	VMware 50
Dataram 58	GroupLogic 53	STEC 58	WiebeTech 55
Drobo 50	Micron Technology 58	Texas Memory Systems 50, 57	XIO Storage 58
Ensim 50	NewsGator Technologies 54		

DIRECTORY OF SERVICES | WINDOWS IT PRO NETWORK

Search our network of sites dedicated to hands-on technical information for IT professionals.
www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.
www.windowsitpro.com/go/forums

News

Check out the current news and information about Microsoft Windows technologies.
www.windowsitpro.com/go/news

EMAIL NEWSLETTERS

Get free news, commentary, and tips delivered automatically to your desktop.

DevProConnections UPDATE
Exchange & Outlook UPDATE
Security UPDATE
SharePoint Pro UPDATE
SQL Server Magazine UPDATE
Windows IT Pro UPDATE
WinInfo Daily UPDATE

www.windowsitpro.com/email

RELATED PRODUCTS

Custom Reprint Services

Order reprints of *Windows IT Pro* articles:
reprints@pentonreprints.com

Windows IT Pro VIP

Get exclusive access to over 40,000 articles and solutions on CD and via the Web. Includes FREE access to eBooks and archived eLearning events, plus a subscription to either *Windows IT Pro* or *SQL Server Magazine*.
www.windowsitpro.com/go/vipsub

SQL SERVER MAGAZINE

Explore the hottest new features of SQL Server, and discover practical tips and tools.
www.sqlmag.com

ASSOCIATED WEBSITES

DevProConnections

Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at DevProConnections.com, where IT pros creatively and proactively drive business value through technology.
www.devproconnections.com

SharePoint Pro

Dive into Microsoft SharePoint content offered in specialized articles, member forums, expert tips, and web seminars mentored by a community of peers and professionals.
www.sharepointpromag.com

NEW WAYS TO REACH *WINDOWS IT PRO* EDITORS:

LinkedIn: To check out the *Windows IT Pro* group on LinkedIn, sign in on the LinkedIn homepage (www.linkedin.com), select the Search Groups option from the pull-down menu, and use "Windows IT Pro" as your search term.

Facebook: We've created a page on Facebook for *Windows IT Pro*, which you can access at: http://tinyurl.com/d5bquf. Visit our Facebook page to read the latest reader comments, see links to our latest web content, browse our classic cover gallery, and participate in our Facebook discussion board.

Twitter: Visit the *Windows IT Pro* Twitter page at www.twitter.com/windowsitpro.

Windows IT Pro

Ctrl+Alt+Del

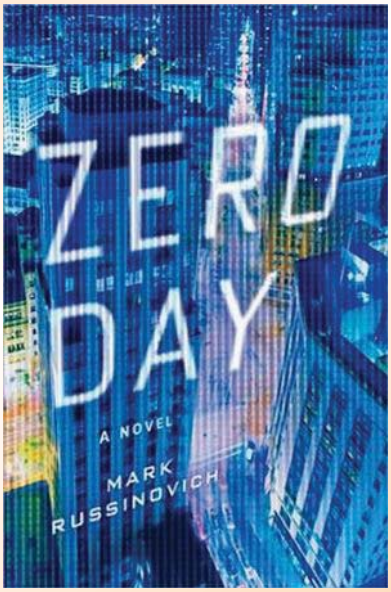
by Jeff James

"Send your funny screenshots, oddball product news, and hilarious end-user stories to rumors@windowsitpro.com. If we use your submission, you'll receive a *Windows IT Pro* Rubik's Cube."

Mark Russinovich's *Zero Day*

This is shaping up to be a banner year for cybersecurity news of all stripes. I've already posted about the havoc that Anonymous and Lulzsec have caused, the discovery of an "indestructible" botnet, and how universities (and end users) are struggling with security issues. Then there was Stuxnet, a complex bit of malware that was believed to have been jointly developed by American and Israeli intelligence services to attack Siemens industrial equipment used in the Iranian nuclear program.

Against this backdrop of security vulnerabilities, Microsoft Technical Fellow (and *Windows IT Pro* Senior Contributing Editor) Mark Russinovich recently authored *Zero Day*, a novel focused on the real-world threat of cyberterrorism. Although *Zero Day* is fiction, the premise that Russinovich presents—that cyberterrorism is real, and that it's only a matter of time before a terrorist group chooses this option—is a terrifying one to consider.



The first few chapters of *Zero Day* focus on a series of devastating attacks by a new breed of malware that's causing pilots to lose control of their aircraft, making hospital record systems fail, disrupting robotic auto assembly lines, and causing nuclear power plants to fail.

That's when protagonist Jeff Aiken enters the scene. Something of a lone-wolf computer security genius, Aiken has turned in his security passcard at the CIA to escape some suffocating government bureaucracy and, to some extent, flee from personal demons and do some soul-searching after his wife's death during 9/11. Now working as a freelance computer security expert, Aiken makes a comfortable living selling his services to the highest bidder.

Aiken rolls up his sleeves and comes to the aid of Fischerman, Platt & Cohen, a small Manhattan legal firm that has seen its expensive PCs turned into glorified paperweights by a mysterious cyberattack. Aiken starts working with Sue Tabor, an overworked and under-appreciated (surprise!) systems administrator, in an effort to solve the mystery.

The first half of the novel is a bit slow going, but the pace gradually gathers steam admirably. Aiken soon joins forces with Dr. Daryl Haugen, a statuesque blonde who just happens to be an old friend and security expert at the Department of Homeland Security (DHS). Haugen soon becomes Aiken's love interest, and the plot thickens from there.

Zero Day includes references to many real-world cyberattacks. In one section, Russinovich also alludes to some of his own work around discovering Sony's use of rootkits in their music CDs a few years ago. *Zero Day* excels in its technical aspects, and it's here where Russinovich displays his mastery of (and intimate familiarity with) specific cybersecurity terms and technology. Less tech-minded readers might gloss over these parts, but IT professionals, systems administrators, and other tech-savvy readers—myself included—will find these portions of the novel some of the most enjoyable.

Zero Day is Russinovich's first work of fiction, and some aspects of the book seem a bit unpolished; some of the dialogue is awkward and stilted in spots, and I found reading through a chapter devoted to an extensive, vowel-deficient IM exchange a bit tedious. Russinovich isn't Robert Ludlum, and Jeff Aiken most definitely isn't Jason Bourne, but Russinovich seems to channel both at various points. That isn't entirely a bad thing, as Russinovich has managed to blend some thrilling, dramatic action with a host of specific technical detail that makes *Zero Day* a thoroughly engaging read.

My gripes are minor; this is one of the best books I've read this year, and arguably one of the most readable novels ever written about cyberterrorism. It's exceptionally impressive considering that it's Russinovich's first novel. It also won't be his last: Russinovich told me during an interview on the Microsoft campus in early September that he's already working on *Trojan Horse*, a sequel to *Zero Day* that will be published by St. Martin's Press in 2012.

InstantDoc ID 140670

November 2011 issue no. 207, *Windows IT Pro* (ISSN 1552-3136) is published monthly. *Windows IT Pro,* 748 Whalers Way, Fort Collins, CO 80525, (800) 793-5697 or (970) 663-4700. Sales and Marketing Offices: 748 Whalers Way, Fort Collins, CO 80525. Advertising rates furnished upon request. Periodicals Class postage paid at Fort Collins, Colorado, and additional mailing offices. **POSTMASTER: Send address changes to *Windows IT Pro,*** 748 Whalers Way, Fort Collins, CO 80525. **SUBSCRIBERS:** Send all inquiries, payments, and address changes to *Windows IT Pro,* Circulation Department, 748 Whalers Way, Fort Collins, CO 80525. Printed in the USA.

LOVE your AV

New Version 5.0

VIPRE 5.0 was built with IT admins in mind

VIPRE provides powerful protection against virus and malware threats without slowing down your PCs. Version 5.0 features the latest in detection technologies, and is easy to install, easy to deploy and easy to manage. Try VIPRE today and love your AV.

- » High-performance endpoint security
- » Industry-leading malware detection
- » Intuitive, centralized management console
- » Affordable for organizations of all sizes
- » The best tech support in the business

VIPRE® AntivirusBusiness

For your free 30-day trial, visit:

www.loveyourav.com

tel: 1 (888) 688-8457 | fax: 1 (727) 562-5199 | email: vipresales@gfi.com | ***www.gfi.com***

GFI®

Microsoft

Team members in three time zones.
One document in the cloud.
A single place for all information.
It all works together.

Introducing Microsoft Office 365. Collaborate in the cloud with Office, Exchange, SharePoint, and Lync videoconferencing. **Starting as low as $10 per user per month. Begin your free trial now at Microsoft.com/office365**

Scan tag with a smartphone to learn about the Office 365 free trial.
Download the free scanner app at http://gettag.mobi

Microsoft® Office 365